VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Berlekampův algoritmus

Berlekamp's algorithm

2020 Lukáš Růžička

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Zadání bakalářské práce

Student:	**Lukáš Růžička**
Studijní program:	B2647 Informační a komunikační technologie
Studijní obor:	1103R031 Výpočetní matematika
Téma:	Berlekampův algoritmus Berlekamp´s algorithm
Jazyk vypracování:	čeština

Zásady pro vypracování:

Berlekampův algoritmus slouží jako nástroj pro rozklad polynomů nad konečnými tělesy na ireducibilní polynomy. Schopnost nalézat ireducibilní polynomy a rozkládat prvky konečných těles je využívána v teoretických i praktických aplikacích teorie kódování a šifrování.
Bakalářská práce by měla popisovat teoretické základy Berlekampova algoritmu, a měla by obsahovat množství řešených příkladů využitelných jako studijní materiály. Autor by se měl také pokusit vytvořit funkční aplikaci, která by faktorizovala daný polynom nad daným konečným tělesem Z p[x].

Seznam doporučené odborné literatury:

Lidl R., Niederreiter H. : Introduction to Finite Fields and their Applications. Cambridge: Cambridge University Press, 1994
Lidl R., Pilz G. : Applied Abstract Algebra. New-York, Springer-Verlag, 1997
Gallian J.A. : Contemporary abstract algebra. Boston, Brooks/Cole, 2013

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **RNDr. Pavel Jahoda, Ph.D.**

Datum zadání: 01.09.2019
Datum odevzdání: 30.04.2020

prof. RNDr. Jiří Bouchala, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Praze 30. dubna 2019 …… ……

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava.

V Ostravě 15. května 2020 .....

Prvně bych chtěl poděkovat svému školiteli, RNDr. Pavlu Jahodovi, Ph.D, za vedení této bakalářské práce. Druhak patří dík mnoha dalším lidem za neutuchající podporu a povzbuzování, za čtení a korekce textu, apd.: Máše Palasové, Martinu Vacovskému, Karolíně Genzové, tátovi („Co bakalářka?!“), mámě („To bude dobrý!“), babičce („Co diplomka?!“), ...

Abstrakt

Tato práce popisuje Berlekampův algoritmus, který slouží k rozkladu polynomů nad konečnými tělesy na ireducibilní faktory. Konečné těleso má mnoho zajímavých vlastností, ať už některé sdílí s celými, reálnými i komplexními čísly, a naopak mnoho unikátních - které oproti nekonečným tělesům umožňují existenci Berlekampova algoritmu.

Klíčová slova: Berlekampův algoritmus, faktorizace, polynom, konečné těleso

Abstract

This thesis describes Berlekamp's algorithm, which factors polynomials over finite fields into ireducible ones. Finite field has many interesting properties, either in common with integers, real or complex numbers, andr many other unique ones - that in contrast with infinite fields allow existence & correctness of Berlekamp's algorithm.

Key Words: Berlekamp's algorithm, factorization, polynomial, finite field

Obsah

Seznam použitých zkratek a symbolů

$\mathbb{N}$	–	Přirozená čísla
$\mathbb{N}_0$	–	Přirozená čísla včetně 0
$\mathbb{Z}$	–	Celá čísla
$\mathbb{Q}$	–	Racionální čísla
$\mathbb{R}$	–	Reálná čísla
$\mathbb{P}$	–	Množina všech prvočísel
$A \subset\subset B$	–	A je podgrupa/podokruh B
$\mathcal{P}(A)$	–	Potenční množina A
$a \mid b$	–	a dělí b
$a \nmid b$	–	a nedělí b
$\mathbb{F}$	–	Těleso
$\mathbb{F}_q$	–	Konečné těleso řádu q

1 Úvod

Tato práce se zabývá Berlekampovým algoritmem, který slouží jako nástroj pro rozklad polynomů nad konečnými tělesy na ireducibilní polynomy. Schopnost nalézat ireducibilní polynomy a rozkládat prvky konečných těles je využívána v teoretických i praktických aplikacích teorie kódování a šifrování.

2 Potřebná teorie

Vzhledem k povaze zadání této práce bude mnoho definic uvedeno ve specializované formě, stejně tak u tvrzení by mnohdy šlo slevit z některých předpokladů a získat obecnější výsledek.

2.1 Vlastnosti přirozených/celých čísel

Následují vybraná tvrzení týkající se příhodných vlastností celých čísel. Není kladen žádný důraz na definici všech využívaných pojmů, neboť jsou „elementární“ a „všeobecně známé“:

Definice 1 (Dělitelnost) *[3, d. 33] Nechť $k, l \in \mathbb{Z}$. Řekneme, že k **dělí** l, psáno $k \mid l$, pokud existuje $n \in \mathbb{Z}$ takové, že $l = kn$. V opačném případě nazveme čísla k, l nesoudělná a píšeme $k \nmid l$.*

Věta 1 (Dělení se zbytkem) *[3, v. 22] Nechť $c, d \in \mathbb{Z}, d \neq 0$. Pak existují $q, r \in \mathbb{Z}$ taková, že $c = dq + r$ a $0 \leq r < |d|$.*

Definice 2 (Největší společný dělitel) *[3, d. 33, v. 23] Nechť máme $a, b \in \mathbb{Z}$. Pak $d \in \mathbb{Z}$ nazveme **největším společným dělitelem** čísel a, b, značíme $\gcd(a, b) = d$, pokud*

$$d \mid a \wedge d \mid b \wedge (\forall c \in \mathbb{Z} : c \mid a \wedge c \mid b \Rightarrow c \mid d) \tag{2.1}$$

Věta 2 (Bézoutova) *[2, t. 1.8, t. 4.3] Nechť jsou $a, b \in \mathbb{Z}$, $d = \gcd(a, b)$. Pak*

$$\exists u, v \in \mathbb{Z} : ua + vb = d. \tag{2.2}$$

Množina všech těchto párů je nekonečná, a sestává z $(u + k\frac{b}{\gcd(a,b)}, v - k\frac{a}{\gcd(a,b)})$ pro jakýkoliv pevně zvolený pár (u, v) a $\forall k \in \mathbb{Z}$. Vždy obsahuje 2 význačné prvky s touto vlastností:

$$|u| \leq |\frac{b}{\gcd(a, b)}| \wedge |v| \leq |\frac{a}{\gcd(a, b)}| \tag{2.3}$$

Příklad 1
Pro $\forall p \in \mathbb{P}$ a $\forall n \in \{1, \ldots, p-1\}$ platí $\gcd(p, n) = 1$, takže podle 2:

$$\exists u, v \in \mathbb{Z} : up + vn = 1$$

Navrch ještě existuje právě jedno v takové, že $v \in \{1, \ldots, p-1\}$. Tato vlastnost se později bude hodit. ∎

Definice 3 (Kongruence) *Nechť jsou $x, y \in \mathbb{Z}, n \in \mathbb{N}$. Pak x a y nazveme **kongruentní modulo** n, píšeme $x \equiv y \mod n$, pokud $\exists k \in \mathbb{Z} : x = y + kn$, neboli $n \mid (x - y)$.*

Věta 3 (Čínská zbytková) *[2, t. 2.6] Nechť $n_1, \ldots, n_k$ jsou vesměs po dvou nesoudělná přirozená čísla, $a_1, \ldots, a_k \in \mathbb{Z}$ libovolná. Potom*

$$(\exists a \in \mathbb{Z})(\forall i \in \{1, \ldots, k\} : a \equiv a_i \mod n_i)$$

Různých řešení a' existuje nekonečně mnoho, a všechny splňují následující rovnici:

$$a \equiv a' \mod n$$

při označení $n = n_1 \cdot \ldots \cdot n_k$.

2.2 Základní pojmy algebry

2.2.1 Grupa

Definice 4 *Nechť M je neprázdná množina $a \cdot : M \times M \to M$ binární operace s těmito vlastnostmi:*

- $\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- $\exists\, \mathrm{e} \in M : \forall a \in M : a \cdot \mathrm{e} = \mathrm{e} \cdot a = a$, *toto* e *nazýváme neutrálním prvkem,*
- $(\forall a \in M)(\exists b \in M : a \cdot b = b \cdot a = \mathrm{e})$, *toto b nazveme prvkem inverzním k prvku a. Budeme jej značit $a^{-1} \overset{ozn.}{=} b$,*

*pak se dvojice $(M; \cdot)$ nazývá **grupa**. Pokud navrch pro $\forall a, b \in M : a \cdot b = b \cdot a$, neboli platí komutativní zákon, říkáme jí **Abelova**. Označme $G = (A; \cdot)$ - pokud nebude uvedeno jinak, zápisem $x \in G$ je myšleno $x \in A$ a obdobně se všemi ostatními množinovými operacemi.*

Věta 4 *Nechť G je Abelova grupa, pak* e *je unikátní. Dále ke každému $a \in G$ existuje právě jeden prvek inverzní.*

Existují dva příhodné zápisy operace na prvcích Abelovy grupy $G = (M; \cdot)$:

1. aditivní - přeznačme operaci $\cdot$ na $+$, neutrální prvek na $\mathbf{0}$, inverzi k $a \in G$ na $-a$, $\underbrace{a + a + \ldots + a}_{n\text{krát}}$ na $n \times a$ - nebude-li hrozit zmatení, pak na pouhé na;
2. multiplikativní - pokud nemůže dojít ke zmatení, $a \cdot b$ se zapisuje jakožto ab, neutrální prvek se značí $\mathbf{1}$, $a^n \overset{ozn.}{=} \underbrace{a \cdot a \cdot \ldots \cdot a}_{n\text{krát}}$ pro $\forall a, b \in G$, $\forall n \in \mathbb{N}_0$.

Například $(\mathbb{Z}; +)$ je Abelova grupa pro standartní sčítání celých čísel. Zajímavější jsou ale následující dvě grupy pro libovolné pevně zvolené prvočíslo p:

1. $Z_p := (\{0, \ldots, p-1\}; +)$ kde se sčítá modulo p,

2. $Z_p^* := (\{1, \ldots, p-1\}; \cdot)$ s násobením modulo p. Existence (a jednoznačnost) inverzního prvku je důsledek 1 - při zde uvedeném značení je k n inverzní prvek roven v.

Definice 5 *Nechť G je Abelova grupa. Nazveme ji **konečnou**, pokud $|G| \in \mathbb{N}$, a jejím **řádem** pak myslíme tento počet prvků. V opačném případě ji nazveme **nekonečnou**. Dále buď $a \in G$. Pak*

- ***řádem prvku** a myslíme číslo $|a| := \min\{k \in \mathbb{N} : a^k = \mathrm{e}\}$. Pokud ale takové číslo neexistuje, říkáme, že a má nekonečný řád.*
- *Pokud všechny prvky mají konečný řád, dáme grupě přízvisko periodická.*

Definice 6 *Nechť G je Abelova grupa, $\emptyset \neq N \subseteq G$. Pak N se nazývá **uzavřená** v grupě G, pokud $\forall a, b \in N : ab^{-1} \in N$.*

V grupě $(\mathbb{Z}; +)$ je například množina všech sudých čísel uzavřená, množina všech lichých čísel ale nikoliv - rozdíl (to jest druhým sčítancem je nějaký inverzní prvek) dvou lichých čísel je číslo sudé.

Poznámka 1 Nechť $G = (M; \cdot)$ je Abelova grupa, N je uzavřená v G. Pak $H := (N; \cdot)$ je také Abelova grupa kterou nazveme **podgrupou** G, a značíme $H \subset\subset G$ nebo alternativně, pokud nemůže dojít ke zmatení, $N \subset\subset G$.

Definice 7 *Nechť G Abelova grupa, $N \subseteq G$. Pak $\langle N \rangle \overset{ozn.}{=} (\bigcap\{H : H \subset\subset G \wedge N \subseteq H\}; \cdot)$ se nazývá **podgrupa** G **generovaná množinou** N. Existuje-li $B \subseteq G$ taková, že $\langle B \rangle = G$, nazveme B **množinou generátorů** grupy G. Pokud $|B| \in \mathbb{N}$, pak říkáme, že G je **konečně generovaná**.*

2.2.2 Kongruence

Na začátek si připomeneme definici relace ekvivalence [2, str. 15], zbytek je vesměs výtah z [3, kap. 16].

Definice 8 (Relace ekvivalence) *Nechť M je množina $a \equiv$ binární relace na M. Pak $\equiv$ nazveme **ekvivalencí** na M, pokud:*

1. $\forall a \in M : a \equiv a$,
2. $\forall a, b \in M : a \equiv b \Leftrightarrow b \equiv a$,
3. $\forall a, b, c \in M : a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$.

*Systém množin $M/_{\equiv} := \{T_a \subseteq M : a \in M \wedge (b \in T_a \Leftrightarrow a \equiv b)\} \subset \mathcal{P}(M)$ se nazývá **rozklad množiny** M **podle ekvivalence** $\equiv$.*

Poznámka 2 Pro $\emptyset \neq M$ množinu a $\equiv$ ekvivalenci na M platí: $\forall a, b \in M : T_a = T_b \Leftrightarrow a \equiv b$.

Definice 9 (Kongruence a faktorgrupa) *Nechť je $G = (M; \cdot)$ Abelova grupa a $\equiv$ ekvivalence na M. Pak tuto ekvivalenci nazveme **kongruencí** na G, pokud*

$$\forall a, b, c, d \in M : (a \equiv b \wedge c \equiv d) \Rightarrow ac \equiv bd. \tag{2.4}$$

*Pro takovouto ekvivalenci definujeme binární operaci $\bullet : M/_{\equiv}{}^2 \to M/_{\equiv}$ tak, že $T_a \bullet T_b = T_{ab}$. Potom $G/_{\equiv} \overset{def.}{=} (M/_{\equiv}; \bullet)$ se nazývá **faktorgrupa** G. Nadále budeme značit operaci $\bullet$ faktorgrupy stejně jakžto operaci $\cdot$ jeho grupy.*

Na celých číslech jsme definovali kongruenci v 3. Pro fixní $n \in \mathbb{Z}$ je to zároveň i kongruence ve smyslu 9 pro grupu $(\mathbb{Z}; +)$:

Nechť pro $a, b, c, d \in \mathbb{Z}$ platí $a \equiv b \mod n \wedge c \equiv d \mod n$, neboli existují $k, l \in \mathbb{Z}$ taková, že $a = b + kn \wedge c = d + ln$. Pak ovšem $ac = bd + (\underbrace{bl + kd + kl}_{\in\mathbb{Z}})n$, takže $ac \equiv bd \mod n$. Množina T_a sestává ze všech celých čísel, jež mají stejný zbytek po dělení číslem n.

Definice 10 *Nechť G je Abelova grupa, $H \subset\subset G$. Definujme ekvivalenci na G podle H, značenou $\equiv_H$, takto: $a \equiv_H b \Leftrightarrow ab^{-1} \in H$; rozkladovou třídu ekvivalence obsahující prvek $a \in G$ označíme T_a^H.*

Správně by se mělo dokázat, že relace definovaná v 10 je doopravdy ekvivalence - to lze najít v [3, kap. 17]. Dále platí, že $H = T_{\mathrm{e}}^H$.

Příklad 2
Vezměme si libovolné prvočíslo p - množina $p\mathbb{Z} \overset{def}{=} \{pk : k \in \mathbb{Z}\}$ sestává ze všech jeho násobků. Definujeme-li pomocí ní kongruenci, množina T_a - prvek faktorgrupy $\mathbb{Z}/_{p\mathbb{Z}}$ - sestává přesně ze všech celých čísel majících po dělení prvočíslem p stejný zbytek, pro zjednodušení jej označme $[a]_p \overset{def.}{=} T_a$. ∎

2.2.3 Rozklad grupy

Tato podsekce shrnuje [3, kap. 17]:

Definice 11 *Nechť máme $G = (M; \cdot)$ grupu. Libovolnou podmožinu M nazveme **komplexem**. Součin komplexů definujeme následovně: $\forall A, B \in \mathcal{P}(M) : AB \overset{ozn.}{=} \{ab \in M : a \in A \wedge b \in B\}$. Pro zkrácení zápisu klademe $aB \overset{ozn.}{=} \{a\}B, Ab \overset{ozn.}{=} A\{b\}$, pro libovolná $a, b \in M$.*

Věta 5 *Nechť G je Abelova grupa, $H \subset\subset G$. Pak $\forall a \in G : T_a^H = aH$.*
Důkaz *Buď $x \in T_a^H$: $x \equiv_H a \Leftrightarrow xa^{-1} \in H \Leftrightarrow \exists h \in H : h = xa^{-1} \Leftrightarrow x = ah \Leftrightarrow x \in aH$.* ∎

Věta 6 *Budiž G Abelova grupa, $H \subset\subset G$. Pak všechny třídy libovolné ekvivalence na G podle H jsou ekvivalentní množiny, to jest mají stejnou mohutnost.*

Definice 12 *Nechť G je Abelova grupa, $H \subset\subset G$. Pokud existuje číslo $[G:H] := |G/_{\equiv_H}| \in \mathbb{N}$, nazýváme jej **indexem** H **v** G.*

Věta 7 (Lagrangeova) *Nechť G je Abelova grupa, $H \subset\subset G$. Má-li G konečný řád, pak*

$$|G| = [G:H]|H| \tag{2.5}$$

neboli řád libovolné podgrupy dělí řád (konečné) grupy.
Důkaz *Plyne přímo z 6.* ∎

2.2.4 Homomorfismus

Tato kapitola čerpá z [3, kap. 16].

Definice 13 *Nechť $G_1 = (M_1; \cdot_1)$, $G_2 = (M_2; \cdot_2)$ jsou grupy, $h : M_1 \to M_2$. Pokud pro všechna $x, y \in M_1$ platí $h(x \cdot_1 y) = h(x) \cdot_2 h(y)$, pak zobrazení h nazýváme **homomorfismem**. Pokud je navíc zobrazení h*

- *bijekce, nazveme jej izomorfismem,*
- *$G_1 = G_2$, nazveme jej endomorfismem,*
- *izomorfismem a endomorfismem, tak jej nazveme automorfismem.*

Pro zjednodušení budeme občas psát $h : G_1 \to G_2$ a binární operace značit stejně, i když mohou být různé.

Definice 14 *Nechť máme G_1, G_2 grupy, h jejich homomorfismus. Pak množinu*

$$\ker h := \{x \in G_1 : h(x) = \mathrm{e}\}$$

*nazýváme **jádrem homomorfismu** h.*

Věta 8 *Nechť $h : G_1 \to G_2$ je homomorfismem grup. Pak $\ker h$ je uzavřená v G_1.*
Důkaz *Buďte $x, y \in \ker h$: $h(xy) = h(x)h(y) = ee = e$, neboli $h(xy) = e$ takže $xy \in \ker h$.* ∎

Příklad 3
Výše byly zavedeny aditivní grupy $p\mathbb{Z}$ (a z ní plynoucí faktorgrupa $\mathbb{Z}/_{p\mathbb{Z}}$) a Z_p pro $p \in \mathbb{P}$. $\mathbb{Z}/_{p\mathbb{Z}}$ sestává z prvků $[0]_p, [1]_p, \ldots, [p-1]_p$ a je izomorfní s Z_p: onen izomorfismus je následující: $[k]_p$ odpovídá k pro $\forall k \in \{0, 1, \ldots, p-1\}$. Pokud vynecháme nulu, platí totéž i pro násobení: to jest grupa Z_p^* je izomorfní s $\mathbb{Z}^*/_{p\mathbb{Z}^*}$, kde se využilo zjednodušení $\mathbb{Z}^* \overset{ozn.}{=} \mathbb{Z} \setminus \{0\}$. ∎

2.2.5 Cyklické grupy

Tato podsekce je jen shrnutím a specializací [3, kap. 18]

Definice 15 *Nechť máme grupu G, $a \in G$. Pokud $G = \langle a \rangle$, dáme grupě G přízvisko **cyklická**.*

Věta 9 *Nechť $G = (M; \cdot)$ je grupa, $a \in M$ takové, že $G = \langle a \rangle$. Pak platí:*

1. *G je Abelova,*
2. *$G = \{a^k : k \in \mathbb{Z}\}$, což znamená, že nosič libovolné cyklické grupy je nejvýše spočetný,*
3. *libovolné 2 cyklické grupy stejného řádu (popřípadě nekonečné) jsou izomorfní, ba dokonce pokud je G nekonečná, pak je izomorfní s $(\mathbb{Z}; +)$; pokud G má řád $n \in \mathbb{N}$, pak je izomorfní s $E_n = \left(\{\exp(\frac{2k\pi}{n} i) : k \in \mathbb{Z}\}; \cdot\right)$,*
4. *libovolná podgrupa cyklické grupy je sama cyklická.*

Dále předpokládáme, že G má řád $n \in \mathbb{N}$:

1. *pro $\forall k \in \mathbb{N} : k \mid n$ existuje právě jedna podgrupa řádu k,*
2. *pokud naopak $k \in \mathbb{N} : \gcd(k, n) = 1$, pak $G = \langle a^k \rangle$,*
3. *pro $k \in \mathbb{N}, q := \frac{n}{\gcd(n,k)}$ platí $\langle a^k \rangle \subset\subset G$ a má řád roven q.*
4. *pokud $k \in \mathbb{N} : k \mid n$, pak G obsahuje[1] $\varphi(k)$ prvků řádu k.*

Pro nás jsou nejzajímavější Abelovy grupy tvaru Z_p a Z_p^* pro p prvočíslo:

- grupa Z_p sestává z p prvků, takže má $p - 1$ generátorů - libovolné nenulové číslo. Navíc nemá žádné netriviální podgrupy;
- to, že existuje prvek, který sám generuje celý nosič grupy Z_p^*, lze najít v [2, kapitola 11 nebo t. 7.28].

2.3 Okruh, obor integrity a těleso

Definice 16 (Okruh) *[1, def. 1.28] Nechť máme neprázdnou množinu M a dvě binární operace $+, \cdot$ (kde $+$ má menší prioritu než $\cdot$) na ní takové, že $(M; +)$ je Abelova grupa a $(M; \cdot)$ je pologrupa[2]. Nechť dále platí $\forall a, b, c \in M : a(b + c) = ab + ac \wedge (b + c)a = ba + ca$. Pak $R \overset{ozn.}{=} (M; +; \cdot)$ nazveme **okruhem**.*

[1] $\varphi(t)$ je Eulerova funkce - pro přirozené číslo je její hodnota rovna počtu čísel menších než t, jejichž největší společný dělitel s t je roven 1.

[2] Má stejné vlasnosti jako grupa vyjma dvou: není požadována existence neutrálního prvku a inverze.

Zavedmě ještě navrch značení $\mathbf{0}$ *pro neutrální prvek v* $(M;+)$ *nazývaný nulovým prvkem, nebo zjednodušeně nulou, inverzní prvek k* $a \in M$ *vůči* $+$ *budeme značit* $-a$, a^n *pro* $+$ *zapisujme jako* $n \times a$ *- zkrátka a dobře budeme používat „aditivní zápis".*

Pro jednoduchost budeme opět chápat zápis $x \in R$ *jakožto* $x \in M$ *nebude-li uvedeno jinak, stejně tak pro všechny další množinové operace.*

Definice 17 *[1, def. 1.29] Budiž* $R = (M;+;\cdot)$ *okruh. Pokud je*

- R *komutativní a existuje neutrální prvek vzhledem k* $\cdot$ *(zvaný jednička, značený* $\mathbf{1}$*) takový, že* $\mathbf{0} \neq \mathbf{1}$ *a pro* $\forall a, b \in R : ab = \mathbf{0} \Rightarrow a = \mathbf{0} \vee b = \mathbf{0}$ *(neboli neexistují dělitelé* $\mathbf{0}$*), nazveme jej oborem integrity;*
- $(M \setminus \{\mathbf{0}\};\cdot)$ *Abelova grupa, nazveme* R *tělesem. Tělesa budeme značit (nebude-li uvedeno jinak)* $\mathbb{F}$*, případně* $\mathbb{F}_q$ *pokud je jeho nosič konečný a sestává z* q *prvků, a stejně jako v případě grup budeme toto číslo nazývat řádem (tělesa).*

Okruhem je například $(2\mathbb{Z};+;\cdot)$; $(\mathbb{Z};+;\cdot)$ v němž pro operaci $\cdot$ existuje neutrální prvek e $= 1$ je oborem integrity; $(\mathbb{Q};+;\cdot)$, kde pro násobení nejenže existuje neutrální prvek, ale k nenulovému prvku lze i upočíst inverzi, je rovnou tělesem. Z hlediska tohoto textu je ale pro $p \in \mathbb{P}$ nejzajímavější okruh $(Z_p;+;\cdot)$ sestávající z čísel $\{0,\ldots,p-1\}$ s operacemi prováděnými modulo p: má oba neutrální prvky (nulu a jedničku), součin nenulových prvků je nenulový, takže je oborem integrity. Dokonce je ale i tělesem [3, v. 76] - to se dá ukázat dvěma nezávislými způsoby: ke každému prvku $a \in Z_p^*$ existuje a^{-1} (viz 1). Druhým způsobem je aplikace věty 10.

Poznámka 3 (Galoisovo těleso) [1, def. 1.41] Na počest Evarista Galoise se zavádí následující pojmenování: buď $p \in \mathbb{P}$, pak $\mathbb{F}_p \overset{def.}{=} (Z_p;+;\cdot)$ je takzvané **Galoisovo těleso** (řádu p).

Věta 10 *[1, t. 1.31] Pokud je* R *konečný obor integrity, pak je zároveň i tělesem.*
Důkaz *Nechť* $a_1,\ldots,a_n$ *jsou všechny prvky množiny* R^* $(= R \setminus \{\mathbf{0}\})$*. Pak pro libovolné pevně zvolené* $b \in R^*$ *jsou* $ba_1,\ldots,ba_n$ *vzhledem k uzavřenosti* $\cdot$ *opět prvky z* R^* *a navíc jsou všechny vesměs po dvou různé: buďte indexy* $j,k \in \{1,\ldots,n\}$ *takové, že* $ba_i = ba_j$*, pak* $b(a_i - a_j) = \mathbf{0}$*, a vzhledem k tomu, že* R *je obor integrity a* $b \neq \mathbf{0}$*, musí být* $a_i = a_j$*. Vzhledem k tomu, že tedy posloupnost* $ba_1,\ldots,ba_n$ *sestává ze všech nenulových prvků, existuje právě jeden index* l *takový, že* $ba_l = \mathbf{1}$*. To ale znamená, že* $b^{-1} = a_l$*. Z unikátnosti inverzního prvku pak plyne to, že všechny prvky v* R^* *jsou invertibilní.* ∎

2.3.1 Polynomy

Definice 18 *[1, def. 1.48] [3, def. 79] Nechť* $R = (M;+;\cdot)$ *je okruh,* $f := (a_i)_{i=0}^{\infty}$ *posloupnost prvků z* M *taková, že nejvýše konečně mnoho jejích členů je různých od* $\mathbf{0}$*. Potom* f *nazveme* ***polynomem*** *nad* R*.* ***Stupněm polynomu****,* $\mathrm{st}(f)$*, myslíme největší číslo* $k \in \mathbb{N}_0$ *takové, že*

$a_k \neq \mathbf{0}$. *Pokud ale* $f = (\mathbf{0})_{i=0}^{\infty}$, *pak jeho stupeň definitoricky klademe roven* 0, *nazýváme ho* ***nulovým polynomem*** *a značíme* $\boldsymbol{\theta}$.

Je zvykem polynom $f = (a_i)_{i=0}^{\infty}$ zapisovat jakožto formální výraz

$$f(x) = a_0x^0 + a_1x^1 + \cdots = \sum_i a_ix^i$$

kde x je tzv. proměnná/neurčitá - pokud za ní dosadíme libovolný prvek M, dostaneme opět prvek M, chápeme-li v onom výrazu $+, \cdot$ a mocnění jakožto operace z R. Na polynom lze tedy nahlížet i jako na funkci zobrazující z M do M.

Definice 19 *[3, def. 80] Nechť je* $R = (M; +; \cdot)$ *okruh,* $f(x) = \sum_i a_ix^i, g(x) = \sum_i b_ix^i$ *polynomy nad* R. *Pak definujeme na množině všech polynomů následující operace:*

- *rovnost polynomů : polynomy* f, g *jsou si rovny* $\overset{def}{\Leftrightarrow} \forall i \in \mathbb{N}_0 : a_i = b_i$,
- *sčítání polynomů :* $(f \oplus g)(x) = \sum_i (a_i + b_i)x^i$,
- *násobení polynomů :* $(f \odot g)(x) = \sum_i \left(\sum_{k=0}^{i} a_k \cdot b_{i-k} \right) x^i = \sum_i \left(\sum_{\substack{k+l=i \\ k,l \in \mathbb{N}_0}} a_k \cdot b_l \right) x^i$, *kde násobení má standartně větší prioritu než sčítání.*

Zaveďme značení $R[x] = (\text{"množina všech polynomů nad orkuhem } R\text{"}; \oplus; \odot)$ *- lze ukázat, že to je okruh, který budeme nazývat okruhem polynomů nad* R. *Nadále budeme zapisovat operace* $\oplus, \odot$ *jako* $+, \cdot$. *Pokud napíšeme* $f \in R[x]$ *nebo* $f(x) \in R[x]$, *je tím myšlen jeden a ten samý polynom.*

Poznámka 4 Následuje pár tvrzení a konvence:

1. [3, str. 101] V okruhu polynomů je nulou nulový polynom, inverzním prvkem $f = (a_i)_{i=0}^{\infty}$ vzhledem k + je $-f = (-a_i)_{i=0}^{\infty}$.
2. [3, lemma 47 a 48] Nechť R je okruh. Pokud má jedničku, resp. je oborem integrity, resp. násobení komutuje, má tuto vlastnost i okruh polynomů nad ním sestrojený.
3. Pro všechny prvky $a, b \in R$, $A, B \in R[x]$ polynomy takové, že $A(x) = a$, $B(x) = b$ a libovolný polynom $f \in R[x]$ chápeme výraz $a \cdot f(x)$ jakožto $A \cdot f$, $f(x) \cdot a$ jako $f \cdot A$, $b + f(x)$ znamená $B + f$ a konečně $f(x) + b$ značí $f + B$. Obecně řečeno ztotožňujeme konstantní polynomy s prvky definujícího okruhu.

Definice 20 *Nechť* R *je okruh s jedničkou,* $(a_i)_{i=0}^{\infty} \in R[x]$ *nenulový polynom stupně* n. *Pak pokud je* $a_n = \mathbf{1}$, *nazveme tento polynom* ***monickým***.

2.3.2 Podokruh, ideál a faktorokruh

Definice 21 *[1, def. 1.32] Nechť máme $R = (M; +; \cdot)$ okruh, $\emptyset \neq S \subseteq M$. Pak pokud jsou obě operace $+, \cdot$ uzavřené vůči S a $(S; +; \cdot)$ je okruh, nazveme $(S; +; \cdot)$ **podokruhem** R a značíme $(S; +; \cdot) \subset\subset R$, a pokud nemůže dojít ke zmatení, píšeme jednoduše $S \subset\subset R$.*

Dále pro $N \subseteq M$ myslíme okruhem generovaným množinou N následující okruh:

$$\langle N \rangle = \left(\bigcap \{H : H \subset\subset R \wedge N \subseteq H\}; +; \cdot \right) \tag{2.6}$$

Definice 22 (Ideál) *[1, def. 1.33 a 1.35] Nechť máme $R = (M; +; \cdot)$ okruh, $J \subset\subset M$. Platí-li následující výrok : $(\forall a \in M)\ (\forall r \in J : ar \in J \wedge ra \in J)$, nazveme J **ideálem okruhu** R. Pokud je R komutativním okruhem, a existuje $c \in M : J = \langle c \rangle$, nazveme J **hlavním ideálem** R.*

Příklad 4
V $(\mathbb{Z}; +; \cdot)$ je ideálem například podokruh o nosiči $\mathcal{J} = \{pk : k \in \mathbb{Z}\}$ pro libovolné prvočíslo p: $b \cdot \underbrace{pc}_{\in \mathcal{J}} = pbc \in \mathcal{J}$ pro libovolná čísla $b, c \in \mathbb{Z}$. ∎

Poznámka 5 [1, str. 13] Ideál J okruhu $R = (M; +; \cdot)$ je zároveň normální podgrupa aditivní grupy $(M; +)$ - lze pomocí něj definovat kongruenci na celém okruhu - pro všechna $a, b \in M$ definujme $a \equiv b \mod J$, pokud $a - b \in J$. Lze ukázat, že

1. $\forall r, a, b \in M$ taková, že $a \equiv b \mod J$, platí $a + r \equiv b + r \mod J$,
2. $c \equiv d \mod J \wedge a \equiv b \mod J \Rightarrow ca \equiv db \mod J \wedge ac \equiv bd \mod J$,
3. pro $\forall n \in \mathbb{Z}$ a $a \equiv b \mod J$ platí $n \times a \equiv n \times b \mod J$.

Důkaz

První a třetí bod je zřejmý, dokážeme pouze druhý pro komutativní okruh: dozajista existují $j_1, j_2 \in J$ taková, že $a - b = j_1, c - d = j_2$. Pak

$$ac - bd \overset{?}{\in} J \Leftrightarrow \underbrace{aj_2}_{\in J} + ad - bd \overset{?}{\in} J \Leftrightarrow aj_2 + (a - b)d \overset{?}{\in} J \Leftrightarrow aj_2 + \underbrace{j_1 d}_{\in J} \in J$$

a protože ideál je sám o sobě podokruh $(M; +)$, neboli je uzavřený na sčítání, součet je prvkem z J. Tím pádem i úplně první výraz náleží do J, což ale dokazuje postulované tvrzení. ∎

Definice 23 (Faktorokruh) *[1, def. 1.36] Buď $R = (M; +; \cdot)$ okruhem a J jeho ideál. Pak $R/_J$ myslíme okruh $(M/_{\equiv_J}; \oplus; \odot)$ s operacemi definovanými následovně : $\forall a, b \in M$*

- $(a + J) \oplus (b + J) = (a + b) + J$,
- $(a + J) \odot (b + J) = ab + J$.

Operace $\oplus, \odot$ přeznačíme na $+, \cdot$ a $R/_J = (M/_{\equiv_J}; +; \cdot)$ nazveme ***faktorokruhem*** *okruhu R.*

Příklad 5
Pokračování 4: faktorokruh $\mathbb{Z}/_{p\mathbb{Z}}$ se „rozpadá“ na dvě grupy: aditivní, ta je izomorfní s Z_p, a na multiplikativní, která je izomorfní s Z_p^* - pokud z ní „vynecháme“ $\mathbf{0}$. ∎

2.3.3 Homomorfismus okruhů

Definice 24 *Nechť jsou $R_1 = (M_1; +_1; \cdot_1), R_2 = (M_2; +_2; \cdot_2)$ okruhy, $h : M_1 \to M_2$ takové, že $\forall a, b \in M_1 : h(a +_1 b) = h(a) +_2 h(b) \wedge h(a \cdot_1 b) = h(a) \cdot_2 h(b)$. Pak h nazveme* ***homomorfismem*** *R_1 **a** R_2. Množina $\ker h := \{a \in M_1 : h(a) = \mathbf{0}_2 \in M_2\}$, neboli vzor nulového prvku R_2 při zobrazení h, se nazývá* ***jádro homomorfismu*** *h.*

Pokud nebude hrozit zmatení, budeme dolní indexy u operací, neutrálních prvků, apd., vynechávat.

Stejně jako u homomorfismu grup i zde se bijektivní homomorfismus označuje ***izomorfismus****, apd.*

Věta 11 *[3, v. 80] Budiž $R = (M; +; \cdot)$, S okruhy, h jejich homomorfismus. Pak $(\ker h; +; \cdot)$ je ideál v R a $h(R)$ je izomorfní s $R/_{\ker h}$.*

2.3.4 Charakteristika

Pro konečnou grupu je význačný její řád - počet prvků nosiče. Ten je stejně definovaný i pro okruhy, ale s nimi je spojeno navrch ještě jedno význačné číslo:

Definice 25 *[1, def. 1.43] Nechť $R = (M; +; \cdot)$ je okruh. Položme*

$$n := \min\{k \in \mathbb{N} : \forall r \in M : k \times r = \mathbf{0}\},$$

pokud je ale ona množina prázdná, pak definitoricky klademe $n = 0$. Říkáme pak, že okruh R má ***charakteristiku*** *n.*

Věta 12 *[1, t. 1.44 a c. 1.45] Nechť R je konečný obor integrity mající $\mathbf{1}$. Pak jeho charakteristika je prvočíslo.*
Důkaz *Pro spor předpokládejme, že charakteristika k je součin dvou přirozených čísel m, n větších než 1. Pak $\mathbf{0} = k \times \mathbf{1} = (m \times \mathbf{1})(n \times \mathbf{1})$. Neboť jsme v oboru integrity, jeden z činitelů musí být roven $\mathbf{0}$, bez újmy na obecnosti ať je to $m \times \mathbf{1}$. Pak ale pro všechna nenulová $a \in R$ platí $m \times a = m \times (\mathbf{1}\, a) = \underbrace{\mathbf{1}\, a + \ldots + \mathbf{1}\, a}_{m} = (m \times \mathbf{1})a = \mathbf{0}$. Neboť jsme v oboru integrity, nulový součin implikuje alespoň jeden nulový činitel, což vzhledem k volbě a musí být $(m \times \mathbf{1})$. Toto je ale spor s minimálností charakteristiky.* ∎

Pokud máme těleso $(Z_p; +; \cdot)$, jeho aditivní grupa je cyklická a generovaná každým jedním nenulovým prvkem. Má řád právě p, tudíž jeho charakteristika je p.

Poznámka 6 [1, t. 1.46] Nechť R je okruh s charakteristikou $p \in \mathbb{P}$. Pak $\forall a, b \in R, \forall n \in \mathbb{N}$:

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} \tag{2.7}$$

2.3.5 Dělitelnost a ireducibilita

Následuje zobecnění pojmů dělitelnosti a prvočíselnosti dobře známých z přirozených čísel pro komutativní obory integrity s jedničkou:

Definice 26 *[1, str. 17] [3, str. 138]*

Nechť R je tedy komutativní obor integrity s jedničkou, $a, b \in R$. Pak říkáme, že

- *b **dělí** a, psáno $b \mid a$, pokud $\exists c \in R : a = bc$ - v opačném případě se píše $b \nmid a$ a říkáme, že b **nedělí** a,*
- *prvky a, b jsou **asociované**, platí-li $a \mid b \wedge b \mid a$ - v tom případě píšeme $a \parallel b$, v opačném $a \nparallel b$,*
- *pokud je $b \mid a \wedge a \nparallel b$, nazýváme b **vlastním dělitelem** a, pokud ještě $b \nparallel \mathbf{1}$, říkáme mu **netriviální dělitel**,*
- *$p \in R$ je **ireducibilní**, pokud $\forall d \in R : d \mid p \Rightarrow d \parallel \mathbf{1} \vee d \parallel p$.*

Nechť dále J je ideál v R, $J \neq R$. Pokud platí, že

- *$\forall a, b \in R : ab \in J \Rightarrow a \in J \vee b \in J$, pak J nazveme **prvoideálem** v R;*
- *$\forall D$ ideál v $R : J \subset\subset D \Rightarrow J = D \vee D = R$, pak J nazveme **maximálním ideálem** v R;*
- *všechny ideály v R jsou hlavní, to jest $(\forall D$ ideál v $R)(\exists d \in R : D = \langle d \rangle)$, pak R nazveme **oborem hlavních ideálů**.*

Uvedeme zde několik příkladů:

Příklad 6

Mějme okruh $\mathbb{F}_3[x]$, to jest všechny polynomy s koeficienty z tělesa $\mathbb{F}_3$. Platí rovnosti $x^2 = 2 \cdot 2x^2$, neboli $2x^2 \mid x^2$, ale stejně tak i $x^2 \mid 2x^2$, takže jsou zároveň i asociované. Netriviálními děliteli x^2 jsou x a $2x$, vlastními děliteli jsou ještě navrch 1 a 2. Ireducibilní jsou kupříkladu všechny lineární a konstantní polynomy. ∎

Příklad 7

V okruhu $\mathbb{F}_2[x]$ jsou všechny kvadratické polynomy tyto: $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$, všechny lineární $x, x + 1$. Prostým roznásobováním získáme faktorizace všech kvadratických, vyjma posledního - $x^2 + x + 1$ - ten je ireducibilní. ∎

Příklad 8
Nechť $p \in \mathbb{P}$, pak $(p\mathbb{Z}; +; \cdot)$ je jak prvoideál, tak maximální ideál v $(\mathbb{Z}; +; \cdot)$: prvně, každý prvek $m \in p\mathbb{Z}$ je nutně součinem prvočísla p a nějakého přirozeného čísla, neboli je prvoideálem. Za druhé předpokládejme, že $p\mathbb{Z}$ je podokruhem ideálu $J \subset\subset \mathbb{Z}$. Pokud $\exists c \in J \setminus p\mathbb{Z}$, pak podle 2 existují čísla $u, v \in \mathbb{Z}$ taková, že $1 = \underbrace{uc}_{\in p\mathbb{Z} \subset\subset J} + \underbrace{vp}_{\in J}$, což ale znamená, že $J = \mathbb{Z}$ neboť obsahuje **1**. ∎

Věta 13 *[1, t. 1.47] Nechť $R = (M; +; \cdot)$ je komutativní obor integrity s jedničkou, $J \subset\subset R$ je ideál v R. Pak*

- *J je maximálním ideálem v $R \Leftrightarrow R/_J$ je tělesem,*
- *J je prvoideálem v $R \Leftrightarrow R/_J$ je oborem integrity.*

Dále

- *každý maximální ideál v R je zároveň prvoideálem,*
- *pokud je R oborem hlavních ideálů, pak $R/_{\langle c \rangle}$ je tělesem tehdy a jen tehdy, když c je ireducibilní v M.*

Příklad 9
Neboť $(p\mathbb{Z}; +; \cdot)$ je maximální ideál, je faktorokruh $\mathbb{Z}/_{p\mathbb{Z}}$ tělesem. Ten je izomorfní s dříve zavedeným Galoisovým tělesem $\mathbb{F}_p$ - viz 3. ∎

2.4 Polynomy podruhé a blíže

Celá tato podsekce rozvine a přiblíží další vlasnosti polynomů, pomocí kterých se pak definují mnohé užitečné pojmy.

Začneme analogií k dělitelnosti na celých číslech 1 - vesměs je to ale jen opakování 26:

Definice 27 *Nechť $\mathbb{F}$ je těleso, $f, g \in \mathbb{F}[x]$ jsou polynomy, $g \neq \boldsymbol{\theta}$. Pak pokud existuje-li $h \in \mathbb{F}[x]$ takové, že $f = gh$, říkáme, že g **dělí** f, alternativně g **je dělitelem** f a píšeme $g \mid f$.*

Stejně tak lze polynomy dělit se zbytkem1:

Věta 14 *[1, t. 1.52] Nechť $\mathbb{F}$ je těleso, $g \in \mathbb{F}[x]$ nenulový polynom. Pak pro libovolné $f \in \mathbb{F}[x]$ existují jednoznačně určené polynomy $q, r \in \mathbb{F}[x]$ takové, že $f = qg + r$ a navíc $\mathrm{st}(r) < \mathrm{st}(g)$.*
***Důkaz** [2, t. 7.10]* ∎

V předešlém tvrzení je potřeba těleso - například $(\mathbb{Z}; +; \cdot)$ je pouze oborem integrity. Mějme $f, g \in \mathbb{Z}[x]$ takovéto: $f(x) = x^2$, $g(x) = 2x$. Pak pokud by existovaly polynomy q, r výše zmíněných vlastností, muselo by pro vedoucí koeficient u q, označme jej $c \in \mathbb{Z}$, platit, že $2c = 1$, tuto rovnici ale žádné přirozené číslo nesplňuje.

Věta 15 *[1, t. 1.54] Budiž $\mathbb{F}$ těleso. Potom $\mathbb{F}[x]$ je oborem hlavních ideálů, a navíc pro všechny $J \subset\subset \mathbb{F}[x]$, $J \neq \langle \boldsymbol{\theta} \rangle$ ideály, existuje právě jeden monický polynom $g \in \mathbb{F}[x]$ takový, že $J = \langle g \rangle$.*
Důkaz *Buď $g \in J \neq \langle \boldsymbol{\theta} \rangle$ monický polynom nejnižšího možného stupně. Pak pro libovolné $f \in J$ podle 14 existují $q, r \in \mathbb{F}[x]$ takové, že $f = qg + r$. Obě strany rovnosti jsou v J, a stejně tak výraz $f - qg = r$. Vzhledem k tomu, že $\mathrm{st}(r) < \mathrm{st}(g)$, a stupeň g je nejmenší možný, musí být $r = \boldsymbol{\theta}$. Nechť $g_1 \in J$ je monický a generuje J. Pak existují $c_1, c_2 \in \mathbb{F}[x]$ takové, že $g = c_1 g_1$ a $g_1 = c_2 g$, což dává $g = c_1 c_2 g$, takže $c_1 c_2 = \mathbf{1}$. Polynomy jsou stejného stupně, oba dva monické, a jsou si tedy rovny.* ∎

Věta 16 (Největší společný dělitel) *[1, t. 1.55] [2, t. 16.13] Nechť $f_1, \ldots, f_n \in \mathbb{F}[x]$ jsou polynomy a alespoň jeden z nich je různý od $\boldsymbol{\theta}$. Pak existuje právě jeden monický polynom $d \in \mathbb{F}[x]$ takový, že*

- $\forall i \in \{1, \ldots, n\} : d \mid f_i$,
- $(\forall i \in \{1, \ldots, n\})(\forall c \in \mathbb{F}[x] : c \mid f_i \Rightarrow c \mid d)$,
- $\exists b_1, \ldots, b_n \in \mathbb{F}[x] : d = \sum_{i=1}^{n} b_i f_i$.

Definice 28 *Podržme značení z předchozí věty. Polynom d pak nazýváme **největším společným dělitelem** polynomů $f_1, \ldots, f_n$ a značíme $\gcd(f_1, \ldots, f_n) = d$. Je-li $d(x) = \mathbf{1}$, pak soubor $f_1, \ldots, f_n$ nazveme nesoudělným, a pokud navíc $(\forall i, j \in \{1, \ldots, n\})(i \neq j \Rightarrow \gcd(f_i, f_j)(x) = \mathbf{1})$, nazveme soubor $f_1, \ldots, f_n$ po dvou nesoudělným.*

Věta 17 (Čínská zbytková) *[2, t. 16.19] Buďte $f_1, \ldots, f_n \in \mathbb{F}[x]$ po dvou nesoudělné nenulové polynomy, a $g_1, \ldots, g_n \in \mathbb{F}[x]$ libovolné. Označme $f \overset{def.}{=} \prod_{i=1}^{n} f_i$; pak existuje $g \in \mathbb{F}[x]$ takové, že*

$$\forall i \in \{1, \ldots, n\} : g \equiv g_i \mod f_i \tag{2.8}$$

Každé další řešení h splňuje následující podmínku: $h \equiv g \mod f$.

2.4.1 Ireducibilní polynomy

Připomeňme si definici ireducibilního prvku 26 a důležitou větu 13 o tom, kdy je faktorokruh tělesem v kulisách okruhu polynomů:

Definice 29 (Ireducibilní polynom) *[1, d. 1.57] Nechť $f \in \mathbb{F}[x]$ je polynom nenulového stupně. Pak jej nazveme **ireducibilním**, pokud $(\forall a \in \mathbb{F}[x])(a \mid f \Rightarrow f \mid a \vee \mathrm{st}(a) = 0)$.*

Věta 18 *[1, t. 1.61] Nechť $f \in \mathbb{F}[x]$ je polynom. Pak $\mathbb{F}[x]/_{\langle f \rangle}$ je těleso $\Leftrightarrow$ f je ireducibilní.*

Příklad 10
[1, str. 25] Nechť $p \in \mathbb{P}$ a $f \in \mathbb{F}_p[x]$ je ireducibilní polynom stupně $n \in \mathbb{N}_0$. Pak $\mathbb{F}_p[x]/_{\langle f \rangle}$ má řád $q \overset{def.}{=} p^n$. Charakteristika tohoto tělesa je p, jak je kupříkladu jednoduše vidět ze sčítání polynomů. „Sestrojme“ těleso $\mathbb{F}_q$ izomorfní s tímto faktorokruhem:

Vezmeme-li libovolnou třídu G rozkladu $\mathbb{F}_p[x]/_{\langle f \rangle}$ a její libovolný prvek $g \in G$, pak pro unikátně určené $r \in \mathbb{F}_p[x]$, zbytek po dělení polynomu g polynomem f, platí $r + \langle f \rangle = G$. Těleso $\mathbb{F}_q$ sestává ze všech polynomů $\mathbb{F}_p[x]$ se stupněm ostře menším než $\mathrm{st}(f)$. Pokud roznásobením získáme polynom h takový, že $\mathrm{st}(h) \geq \mathrm{st}(f)$, podle 14 existují polynomy $q, r \in \mathbb{F}_p[x]$ takové, že $h = qf + r$. Pak za výsledek operace násobení těchto dvou polynomů považujeme jednoznačně určené r. ∎

2.4.2 Faktorizace polynomu

Rozklad přirozeného čísla na mocniny prvočísel je snad dostatečně znám každému. U polynomů nad (konečnými) tělesy je tomu obdobně, platí zde analogická tvrzení posílená o pár specifických požadavků na činitele - polynomy.

Věta 19 *[1, l. 1.58] [2, kapitola 16.3] Nechť $p \in \mathbb{F}[x]$ je ireducibilní, $f_1, \ldots, f_n \in \mathbb{F}[x]$ jsou libovolné. Pokud $p \mid \prod_{i=1}^{n} f_i$, pak existuje $i \in \{1, \ldots, n\}$ takové, že $p \mid f_i$.*

Důkaz *Platí $\prod_{i=1}^{n} [f_i]_p = [\mathbf{0}]_p$, kde $[g]_p$ je prvek faktorokruhu $\mathbb{F}[x]/_{\langle p \rangle}$, který je tělesem, a o to spíš i oborem integrity, takže v onom produktu musí být jeden z členů roven rozkladové třídě $[\mathbf{0}]_p$, neboli $\exists i \in \{1, \ldots, n\} : p \mid f_i$.* ∎

Věta 20 (Faktorizace) *[1, t. 1.59] Nechť $f \in \mathbb{F}[x]$ je polynom nenulového stupně $\mathrm{st}(f) > 0$. Pak existují (až na pořadí) jednoznačně určené*

1. *'koeficient' $c \in \mathbb{F}$,*
2. *nenulová přirozená čísla $k_1, \ldots, k_n$ taková, že $\sum_{i=0}^{n} k_i \leq \mathrm{st}(f)$,*
3. *a různé monické ireducibilní polynomy $p_1, \ldots, p_n \in \mathbb{F}[x]$*

takové, že $f = c \prod_{i=1}^{n} p_i^{k_i}$.

2.4.3 Kořeny polynomu

Definice 30 *[1, d. 1.63] Nechť $\mathbb{F}$ je těleso, $b \in \mathbb{F}$ a $f \in \mathbb{F}[x]$, $\boldsymbol{\theta} \neq f = (a_i)_{i=0}^{\infty}$. Pak b nazveme **kořenem** polynomu f tehdy a jen tehdy, pokud $\sum_{i=0}^{\mathrm{st}(f)} a_i b^i = \mathbf{0}$.*

Věta 21 *[1, t. 1.64] Budiž $f \in \mathbb{F}[x]$, $f \neq \boldsymbol{\theta}$. Pak $b \in \mathbb{F}$ je jeho kořenem $\Leftrightarrow (x - b) \mid f(x)$.*

Důkaz *Z 14 získáme polynomy $q \in \mathbb{F}[x]$ a „koeficient“ $c \in \mathbb{F}[x]$ - konstantní polynom - pro které platí: $f(x) = q(x)(x-b)+c$. Dosazením b získáme $c = f(b)$. Pokud je tedy b kořenem, $(x-b) \mid f$, a naopak, ona proklamovaná dělitelnost implikuje $f(b) = c = \mathbf{0}$.* ∎

Poznámka 7 Polynom stupně alespoň 2 s koeficienty z nějakého tělesa nemůže být ireducibilní pokud má nějaký kořen.

Definice 31 *[1, d. 1.65] Nechť $f \in \mathbb{F}[x]$ je nenulový polynom, $b \in \mathbb{F}$ jeho kořen. Pak $k \in \mathbb{N}$ nazveme **násobností** kořene b polynomu f, pokud $(x-b)^k \mid f(x) \wedge (x-b)^{k+1} \nmid f(x)$.*

Věta 22 *[1, t. 1.66] Budiž $f \in \mathbb{F}[x]$, $\mathrm{st}(f) \geq 0$ a $(b_1, k_1), \ldots, (b_n, k_n) \in \mathbb{F} \times \mathbb{N}$ jsou všechny dvojice kořenů f spolu s jejich násobnostmi. Pak $\prod_{i=1}^{n} (x-b_i)^{k_i} \mid f(x)$ a $\sum_{i=1}^{n} k_i \leq \mathrm{st}(f)$, neboli f může mít nanejvýš n různých kořenů v $\mathbb{F}$.*

2.5 Rozšíření tělesa

Touto podsekcí počínaje, jeden z úkolů do konce sekce je následující: uvést argumenty z nichž vyplyne, že libovolná dvě konečná tělesa o stejném počtu prvků jsou izomorfní.

Věta 23 *[2, t. 7.7] Nechť $\mathbb{F}_q$ je konečné těleso řádu $q \in \mathbb{N}$. Pak existuje $w \in \mathbb{N}$ takové, že $q = p^w$, kde p je charakteristika $\mathbb{F}_q$, tedy prvočíslo.*

Jen pro připomenutí:

Poznámka 8 Nechť $\mathbb{F}$ je těleso, $S \subset\subset \mathbb{F}$ jeho podokruh, takže S je také tělesem. Pak říkáme, že $\mathbb{F}$ je rozšířením tělesa S. Pokud je $S \neq \mathbb{F}$, pak S nazýváme vlastním podtělesem tělesa $\mathbb{F}$, jinak nevlastním.

Definice 32 *[1, d. 1.77] Buď $\mathbb{F}$ těleso. Pokud nemá žádné vlastní podtěleso, pak $\mathbb{F}$ nazveme **prvotělesem**.*

Věta 24 *[1, t. 1.78] Nechť $\mathbb{F}$ je konečné těleso, $S \subset\subset \mathbb{F}$. Pokud je S prvotěleso, pak charakteristika $\mathbb{F}$ je rovna $p \in \mathbb{P} \Rightarrow S$ je izomorfní s $\mathbb{F}_p$.*
Důkaz *[3, pod definicí 98]* ∎

Například $\mathbb{F}_p$ pro libovolné prvočíslo p je prvotěleso. Dále pro f ireducibilní polynom s koeficienty z $\mathbb{F}_p$ je $\mathbb{F}_p[x]/_{\langle f \rangle}$ těleso. Jeho prvotělesem je množina polynomů nulového stupně, která je izomorfní s $\mathbb{F}_p$.

Definice 33 *[1, d. 1.79 a 1.80] Buďte $\mathbb{F} = (A; +; \cdot)$ těleso, S jeho podtěleso a $M \subseteq A$. Pak **rozšířením** S o M myslíme $S(M) := (\bigcap\{K : K \subset\subset \mathbb{F} \wedge S \cup M \subseteq K\}; +; \cdot)$. Sestává-li M z prvků*

$\{a_1, \ldots, a_n\}$, *píšeme* $S(a_1, \ldots, a_n)$ *místo* $S(M)$*; pokud je pouze* $M = \{m\}$*, nazýváme* $S(m)$ *jednoduchým rozšířením* S *a prvku* m *dáváme přízvisko definující.*

Nechť dále $\theta \in \mathbb{F}$*. Pak pokud* $\exists f \in S[x]$*,* $f(x) = a_0 + a_1 x + \cdots + a_n x^n$*, nenulový polynom takový, že* $f(\theta) = a_0 + a_1\theta + \ldots + a_n\theta^n = \mathbf{0}$*, říkáme, že* θ *je* ***algebraická*** *v* S*.*

Definice 34 *[1, d. 1.81] Nechť* $\mathbb{F}$ *je těleso,* S *jeho podtěleso a* $\theta \in \mathbb{F}$ *je algebraická v* S*. Pak monický polynom* g *jednozačně generující hlavní ideál* $J = \{h \in S[x] : h(\theta) = 0\}$ *v* $S[x]$ *nazveme* ***minimálním polynomem*** θ *v* S*.* ***Stupněm*** θ *v* S*, značíme* $\mathrm{st}(\theta)$*, myslíme stupeň jejího minimálního polynomu, to jest* $\mathrm{st}(\theta) \overset{ozn.}{=} \mathrm{st}(g)$*.*

Věta 25 *[1, t. 1.82] Nechť* $\mathbb{F}$ *je těleso,* S *jeho podtěleso,* $\theta \in \mathbb{F}$ *je algebraická v* S *a* $g \in S[x]$ *je minimálním polynomem* θ *v* S*. Pak*

- g *je ireducibilní v* S*,*
- $\forall f \in S[x] : f(\theta) = \mathbf{0} \Leftrightarrow g \mid f$*,*
- g *je monický polynom nejnižšího stupně mající* θ *za kořen.*

Důkaz *Vezměme si ideál* J *z 34. Pak podle 15 platí* $J = \langle g \rangle$*. Kdyby platilo* $g = st$*, a o to spíše* $g(\theta) = s(\theta)t(\theta) = \mathbf{0}$*, pro nekonstantní polynomy* $s, t \in S[x]$*, zákonitě by oba měly stupeň ostře menší nežli* $\mathrm{st}(g)$ *a ten, který má* θ *za kořen, by náležel do* J *- to by byl ale spor s minimalitou stupně* g *podle 15. Všechny polynomy, mající* θ *za kořen, musí být násobkem* g*.* ∎

Poznámka 9 [1, str. 31] Nechť $\mathbb{F} = (M; +; \cdot)$, $K \subset\subset \mathbb{F}$ a $\mathbb{F}$ je rozšířením K. Potom M nad K spolu s operacemi $+$ ("sčítání vektorů") a $\cdot$ ("násobení vektoru skalárem") je vektorový prostor.

Příkladem je, pro f ireducibilní polynom s koeficienty z $\mathbb{F}_p$, těleso $\mathbb{F}_p[x]/_{\langle f \rangle}$ nad $\mathbb{F}_p$.

Definice 35 *[1, d. 1.83] Nechť* $\mathbb{F}$ *je rozšířením* K*. Pak pokud je dimenze* $\mathbb{F}$ *nad* K *konečná, nazveme toto rozšíření* ***konečným*** *a dimenzi* $\mathbb{F}$ *nad* K*, značíme* $\dim_K \mathbb{F}$*, říkáme* ***stupeň*** $\mathbb{F}$ ***nad*** K*.*

Věta 26 *[1, t. 1.85] Nechť* $\mathbb{F}$ *je konečným rozšířením* K*. Pak* $\mathbb{F}$ *je algebraické nad* K*.*
Důkaz *Položme* $n \overset{def.}{=} \dim_K \mathbb{F}$ *a vezměme libovolné* $x \in \mathbb{F} \setminus K$*. Potom ale soubor vektorů* $\{\mathbf{1}, x, \ldots, x^n\}$ *je lineárně závislý, nebo-li existují koeficienty* $a_0, \ldots, a_n \in K$ *takové, že*

$$a_0 + a_1 x + \ldots + a_n x^n = \mathbf{0}$$

což ale s přihlédnutím k 33 dává tvrzení věty. ∎

Věta 27 *[1, t. 1.86] Nechť* $\theta \in \mathbb{F}$ *je algebraická stupně* $n \in \mathbb{N}$ *nad* K*, a nechť* $g \in K[x]$ *je minimální polynom* θ *nad* K*. Potom*

- $K(\theta)$ *je izomorfní s* $K[x]/_{(g)}$,
- $\dim_K K(\theta) = n$ *a* $(\mathbf{1}, \theta, \ldots, \theta^{n-1})$ *je báze* $K(\theta)$ *nad* K,
- $\forall \alpha \in K(\theta) : \alpha$ *je algebraická v* K *a její stupeň* $a \in \mathbb{N}$ *je dělitelem* n, *neboli* $a \mid n$.

Definice 36 *[1, d. 1.90] Nechť* $f \in K[x]$ *polynom,* $n = \mathrm{st}(f) \in \mathbb{N}$ *a* $\mathbb{F}$ *je rozšířením* K. *Pokud existují* $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ *takové, že* $f(x) = a_n(x - \alpha_1) \cdot \cdots \cdot (x - \alpha_n)$, *pak* $K(\alpha_1, \ldots, \alpha_n) \subset\subset \mathbb{F}$ *nazýváme* ***rozkladovým tělesem*** f ***nad*** K.

Věta 28 *[1, t. 1.91] Nechť* $\mathbb{F}$ *je těleso,* $f \in \mathbb{F}[x]$ *a* $\mathrm{st}(f) > 0$. *Pak existuje rozkladové těleso polynomu* f *nad* $\mathbb{F}$, *a navíc libovolná 2 rozkladová tělesa polynomu* f *jsou izomorfní.*

2.6 Vlastnosti konečných těles

Věta 29 *[1, l. 2.1, t 2.2] Nechť* $\mathbb{F}$ *je konečné těleso,* $K \subset\subset \mathbb{F}$ *jeho podtěleso a* $|K| = q \in \mathbb{N}$. *Pak* $|\mathbb{F}| = q^{\dim_K \mathbb{F}}$. *Speciálně nechť* $\mathbb{F}$ *má charakteristikou* $p \in \mathbb{P}$, S *je jeho prvotěleso. Potom pro počet prvků platí* $|\mathbb{F}| = p^{\dim_S \mathbb{F}}$.
Důkaz $\mathbb{F}$ *nad* K *je vektorový prostor konečné dimenze* n. *Má tedy nějakou* n*-člennou bázi a každý jeden prvek* $c \in \mathbb{F}$ *je unikátní lineární kombinací s koeficienty* $c_1, \ldots, c_n$ z K. *Takovýchto různých k-tic koeficientů je* q^n, *což dává první část tvrzení. Prvotěleso konečného tělesa je vždy izomorfní s Galoisovým tělesem řádu* p *podle 24, a z jeho dosazení za* K *do první části tohoto důkazu plyne druhá část tvrzení.* ∎

To znamená, že pro $f \in \mathbb{F}_p[x]$ ireducibilní polynom, $\mathbb{F}_p[x]/_{\langle f \rangle}$ nad $\mathbb{F}_p$ sestává přesně z $p^{\mathrm{st}(f)}$ prvků.

Věta 30 *[1, l. 2.3] Nechť* $\mathbb{F}$ *je konečné těleso s* $q \in \mathbb{N}$ *prvky. Pak* $\forall a \in \mathbb{F} : a^q = a$.
Důkaz *Pro* $a = \mathbf{0}$ *je to jasné, buď tedy* $a \in \mathbb{F}^*$. *To je ale cyklická (multiplikativní) grupa řádu* $q - 1$, *a tudíž platí* $a^{q-1} = \mathbf{1}$. *Vynásobením této rovnosti prvkem* a *získáme tvrzení věty.* ∎

Věta 31 *[1, l. 2.4] Nechť* $\mathbb{F}$ *je konečné těleso s* q *prvky,* K *jeho podtěleso. Potom platí*

$$f(x) = x^q - x = \prod_{d \in \mathbb{F}} (x - d) \tag{2.9}$$

a $\mathbb{F}$ *je rozkladovým tělesem* f *nad* K.
Důkaz *Podle věty 30 pro libovolné* $d \in \mathbb{F}$ *platí* $d^q - d = \mathbf{0}$, *neboli je kořenem polynomu* $x^q - x$, *takže podle 21 platí* $\forall d \in \mathbb{F} : (x - d) \mid (x^q - x)$. *Produkt všech těchto lineárních faktorů je monickým polynomem stupně* q *a musí dělit polynom* $x^q - x$, *který je ale také monický stupně* q, *takže jsou si rovny.*

Z definice rozkladového tělesa je vidět i poslední část tvrzení, neboť $x^q - x$ je polynomem s koeficienty z tělesa K - to z definice musí obsahovat $\mathbf{1}$ *a záporný prvek ke každému svému prvku, tedy i k* $\mathbf{1}$*.* ∎

Nám se bude v následující kapitole velmi hodit toto tvrzení:

Věta 32 *Buď $f \in \mathbb{F}_q[x]$. Pak platí rovnost*

$$f^q(x) - f(x) = \prod_{c \in \mathbb{F}_q} (f(x) - c). \tag{2.10}$$

Důkaz *Neboť pro libovolné $c \in \mathbb{F}_q$ platí $f^q(x) - c^q = (f(x) - c) \sum_{i=0}^{q-1} f^{q-1-i}(x) \cdot c^i$, lze upravit*

$$f^q(x) - f(x) \underbrace{-c^q + c}_{=\mathbf{0}} = (f^q(x) - c^q) - (f(x) - c) = (f(x) - c) \cdot \left(\sum_{i=0}^{q-1} f^{q-1-i}(x) \cdot c^i - \mathbf{1} \right), \tag{2.11}$$

kde jsme ještě navrch využili 30 pro $c^q - c = \mathbf{0}$. Každý člen produktu tedy dělí levou stranu, a zároveň platí $\forall c, d \in \mathbb{F}_q : c \neq d \Rightarrow \gcd(f(x) - c, f(x) - d) = \mathbf{1}$, takže i celý produkt je dělitelem levé strany. Neboť jsou to ale polynomy stejného stupně se stejným koeficientem u nejvyšší mocniny, musí se rovnat. ∎

Následující věty jsou velmi důležité:

Věta 33 *[1, t. 2.5 a 2.6] Nechť $p \in \mathbb{P}, n \in \mathbb{N}$. Pak libovolné těleso S mající p^n prvků je izomorfní s rozkladovým tělesem polynomu $x^{p^n} - x$ nad $\mathbb{F}_p$. Libovolné podtěleso $K \subset\subset S$ má p^m prvků, pro nějaké $m \in \mathbb{N} : m \mid n$, a pokud je $L \subset\subset S$ podtěleso o p^m prvcích, pak $K = L$. Speciálně každé podtěleso $K \subset\subset \mathbb{F}_{p^n}$ o p^m prvcích je rozkladovým tělesem polynomu $f(x) = x^{p^m} - x$ nad $F_p[x]$, to jest jeho nosič sestává ze všech kořenů f (ty jsou všechny z $\mathbb{F}_{p^m}$).*

Tato věta říká, vzhledem k tomu, že složením dvou izomorfismů dostaneme opět izomorfismus, že pro libovolnou mocninu $n \in \mathbb{N}$ libovolného prvočísla p, $q = p^n$, jsou všechna konečná tělesa řádu q izomorfní.

Věta 34 *[1, c. 2.11] Nechť $q, m \in \mathbb{N}$ a $\mathbb{F}_q$ je (konečné) těleso. Pak existuje alespoň jeden ireducibilní polynom $f \in \mathbb{F}_q[x] : \mathrm{st}(f) = m$.*

A konečně, tato věta říká, že pro libovolnou mocninu q prvočísla p a $n \in N$ existuje alespoň jeden ireducibilní polynom s koeficienty z $\mathbb{F}_q$ stupně právě n. S pomocí něj lze pak za pomoci izomorfismu popsaného v 10 sestrojit konečné těleso řádu přesně $w = q^n$. Dokonce lze říct i více:

Věta 35 *[1, t. 3.25] Buď $n \in \mathbb{N}$. Pak počet všech ireducibilních, monických polynomů (stupně právě n) v $\mathbb{F}_q[x]$ je roven*

$$\frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}} \tag{2.12}$$

[1, t. 3.20] Dále produkt všech monických, ireducbilních polynomů, jejichž stupeň je dělitelem čísla n, je roven $x^{q^n} - x$.

Tímto je veškerá potřebná teorie připravena.

3 Algoritmy pro výpočty v konečných tělesech

V přiložené implementaci je Berlekampův algoritmus naprogramován v C++ za použití knihovny Boost [4][3] pro neomezenou aritmetickou přesnost výpočtů s celými čísly. I když u aritmetiky „velkých“ čísel už je složitost algoritmu násobení větší nežli sčítání, apd., v daných algoritmech je pro zjednodušení budeme uvažovat stejné.

Je obecně využíváno „naivních“ algoritmů jak pro aritmetiku čísel, tak i polynomů. Existuje však mnoho efektivnějších algoritmů jak pro násobení čísel, tak polynomů - viz. například [2, kap. 3.5, 3.6, 17.6], avšak jejich popis, odvození a implementace by mnohdy vydalo na samostatnou práci.

Mějme $q, w \in \mathbb{N}$, $p \in \mathbb{P}$ takové, že $q = p^w$. Zajímají nás konkrétně tyto operace v daném konečném tělese $\mathbb{F}_q$: sčítání a opačný prvek, násobení a najití inverze. Co se polynomů z $\mathbb{F}_q[x]$ týká, budou nás opět zajímat sčítání a opačný prvek, násobení, dělení se zbytkem, mocnění modulo nějakým pevně určeným polynomem a největší společný dělitel dvou polynomů.

3.1 Složitost

Jen pro jistotu:

Definice 37 *[2, kap. 3.1] Nechť máme dvě posloupnosti přirozených čísel f, g. Pak pokud existují $n_o \in \mathbb{N}$ takové, že $\forall n \in \mathbb{N} : n > n_0$, a případně ještě reálná čísla $c, d \in \mathbb{R}^+ : 0 < c \leq d$, pak je-li*

- *$f(n) \leq cg(n)$, říkáme, že $f \in \omega(g)$,*
- *$cg(n) \leq f(n) \leq dg(n)$, píšeme $f \in O(g)$,*
- *a konečně, pokud $cg(n) \leq f(n)$, zapisujeme $f \in \Omega(g)$.*

Nechť máme nějaký algoritmus, kde počet operací $f(n)$, které vykoná pro libovolný vstup, jehož komplexita/rozsah/... je „reprezentovatelná“ přirozeným číslem n. Pak o něm řekneme, že má **asymptotickou složitost** $O(g(n))$ pokud $f \in O(g)$, respektive že je zezhora omezen g pokud $f \in \omega(g)$, popřípadě zespoda omezen g, pokud $f \in \Omega(g)$.

Kdykoliv budeme rozebírat v následujících kapitolách složitost algoritmů, bude určena podle přiložené implementace, né podle teoreticky nejlepších známých algoritmů pro danou úlohu.

3.2 Složitost operací v $\mathbb{F}_p$

Pro zjednodušení popíšeme nejdřív algoritmy v tělesech prvků reprezentovaných přirozenými čísly s operacemi „modulo p“.

[3] https://www.boost.org/

3.2.1 Prvky tělesa

Buďte $a, b \in \{0, \ldots, p-1\}$, BÚNO[4] $a \geq b$:

- Sčítání: celá operace sestává ze dvou kroků - sečtení dvou čísel a jejich případnou redukci $\mod p$, z nichž „dražší“ je redukce $\mod p$: [2, t. 3.3] $O(\log(p)(\log(\frac{a}{p})))$. Sečtení je $O(\log(a))$.
- Opačný prvek: prakticky stejné jako sčítání.
- Násobení: [2, t. 3.3] roznásobení $a, b \in \mathbb{F}_p$ zabere $O(\log(a)\log(b))$ operací, redukce $\mod p$ dalších $O(\log(p)\log(\frac{ab}{p}))$.
- Inverzní prvek vůči násobení: za použití rozšířeného Euklidova algoritmu k nalezení a^{-1} vůči $a \in \mathbb{F}_p$ je složitost[2, t. 4.2, 4.4] $O(\log(a)\log(p))$.

3.2.2 Polynomy

Nechť $f, g, d \in \mathbb{F}_p[x]$, BÚNO $\mathrm{st}(g) \leq \mathrm{st}(f)$ a $\mathrm{st}(d) \geq 1$.

- Sčítání: $f + g$ probíhá po složkách - je potřeba $O(\mathrm{st}(g))$ sečtení prvků z $\mathbb{F}_p$.
- Opačný prvek: prakticky stejné jako sčítání.
- Násobení: fg podle 19, [2, kap. 17.1] sestává z $O(\mathrm{st}(f)\,\mathrm{st}(g))$ násobení a sčítání prvků z $\mathbb{F}_p$.
- Dělení se zbytkem: využívá se algoritmu z [2, kap. 17.1]: k získání polynomů $q, r \in \mathbb{F}_p[x]$: $f = qg + r$, viz. 14, je potřeba $O(\mathrm{st}(f) + 1)$ aritmetických operací v $\mathbb{F}_p$.
- Největší společný dělitel: za pomoci Euklidova algoritmu [2, kap. 17.3] je potřeba $O(\mathrm{st}(f)\,\mathrm{st}(g))$ operací v $\mathbb{F}_p$ ke spočtení $d = \gcd(f, g)$.
- Mocnění modulo polynomem d: nechť $e \in \mathbb{N}$. Pak pomocí algoritmu binárního umocňování [2, kap. 3.4, str. 65] lze získat polynom $r \in \mathbb{F}_p[x]$ splňující $f^e \equiv r \mod d$, $\mathrm{st}(r) < \mathrm{st}(d)$ pomocí $O(\log(e)\,\mathrm{st}(d)^2)$ operací v $\mathbb{F}_p$ [2, kap. 17.1, strana 467].

3.2.3 Složitost operací v $\mathbb{F}_q$

Libovolná dvě konečná tělesa stejného řádu jsou izomorfní podle 33, libovolné konečné těleso má charakteristiku $p \in \mathbb{P}$ podle 24 a konečně pro libovolný ireducibilní polynom $f \in \mathbb{F}_p[x]$, stupně právě $n \geq 1$ - jehož existenci zajišťuje 34, bylo sestrojeno 10 konečné těleso $\mathbb{F}_q$ řádu $q = p^n$. Budeme se zabývat operacemi jen v tomto tělese, neboť ostatní stejného řádu jsou s ním izomorfní.

[4] bez újmy na obecnosti

3.2.4 Prvky tělesa

Buďte $a, b \in \mathbb{F}_q$, jsou to tedy polynomy z $\mathbb{F}_p[x]$ stupně ostře menšího než n. BÚNO $\mathrm{st}(a) \geq \mathrm{st}(b)$. Připomeňme ještě, že $f \in \mathbb{F}_p[x]$ je ireducibilní polynom definující současné těleso $\mathbb{F}_q$.

- Sčítání: jedná se o $O(\mathrm{st}(a))$ operací sečtení prvků $\mathbb{F}_p$.
- Opačný prvek: prakticky stejné jako sčítání.
- Násobení: jedná se o roznásobení polynomů a a b, což podle předchozí podsekce vyžaduje $O(\mathrm{st}(a)\,\mathrm{st}(b))$ operací v $\mathbb{F}_p$, a pokud je $\mathrm{st}(ab) \geq \mathrm{st}(f)$, musí se provést redukce modulo polynom f - její cena je $O(\mathrm{st}(a)\,\mathrm{st}(b))$.
- Inverzní prvek vůči násobení: za použití rozšířeného Euklidova algoritmu[2, kap. 17.3 str. 472] k nalezení a^{-1} je potřeba[2, t. 17.5] $O(\mathrm{st}(f)\,\mathrm{st}(a))$ operací v $\mathbb{F}_p$.

3.2.5 Polynomy

Nechť $g, h, d \in \mathbb{F}_q[x]$, BÚNO $\mathrm{st}(h) \leq \mathrm{st}(g)$ a $\mathrm{st}(d) \geq 1$. Vesměs je to opakování stejné podsekce pro polynomiální aritmetiku v $\mathbb{F}_p[x]$.

- Sčítání: $g + h$ probíhá po složkách - je potřeba $O(\mathrm{st}(h))$ sečtení prvků z $\mathbb{F}_q$.
- Opačný prvek: prakticky stejné jako sčítání.
- Násobení: gh podle 19, [2, kap. 17.1] sestává z $O(\mathrm{st}(g)\,\mathrm{st}(h))$ násobení a sčítání prvků z $\mathbb{F}_q$.
- Dělení se zbytkem: využívá se algoritmu z [2, kap. 17.1]: k získání polynomů $q, r \in \mathbb{F}_p[x]$: $g = qh + r$, viz. 14, je potřeba $O(\mathrm{st}(g) + 1)$ aritmetických operací v $\mathbb{F}_q$.
- Největší společný dělitel: za pomoci Euklidova algoritmu [2, kap. 17.3] je potřeba $O(\mathrm{st}(g)\,\mathrm{st}(h))$ operací v $\mathbb{F}_q$ ke spočtení $d = \gcd(g, h)$.
- Mocnění modulo polynomem d: nechť $e \in \mathbb{N}$. Pak pomocí algoritmu binárního umocňování lze získat polynom $r \in \mathbb{F}_q[x]$ splňující $g^e \equiv r \mod d$, $\mathrm{st}(r) < \mathrm{st}(d)$ pomocí $O(\log(e)\,\mathrm{st}(d)^2)$ operací v $\mathbb{F}_q$ [2, kap. 17.1, strana 467].

4 Rozklad polynomu na ireducibilní činitele

V této kapitole se budeme zabývat samotným Berlekampovým algoritmem. Zdroje jsou [1, kapitola 4], [2, sekce 20.3].

Libovolný nenulový polynom lze zapsat jako součin monického a konstantního nenulového polynomu, proto se budeme zabývat pouze monickými polynomy - nechť $f \in \mathbb{F}_q[x]$ je tedy monický polynom. Pak podle věty 20 jej lze zapsat jakožto součin mocnin (monických) ireducibilních polynomů $f_i \in \mathbb{F}_q[x]$. Prvně se nejprve „zbavíme“ faktorů s násobností větší než 1, a až pak budeme rozkládat čtvercoprosté polynomy pomocí proklamovaného Berlekampova algoritmu.

4.1 Rozklad na čtvercoprosté polynomy

Jen pro pořádek:

Definice 38 *Buď $f \in \mathbb{F}_q[x]$. Pak jej nazveme **čtvercoprostým** polynomem, pokud v jeho rozkladu mají všechny ireducibilní činitelé násobnost právě* 1.

Definice 39 (Formální derivace) *[1, d. 1.67] [2, kap. 16.7] Nechť $f = (a_i)_{i=0}^{\infty} \in \mathbb{F}[x]$ je polynomem. Pak **formální derivací** polynomu f nazveme polynom $f' \in \mathbb{F}[x]$ definovaný takto:*

$$f' = ((i+1) \times a_{i+1})_{i=0}^{\infty}.$$

Věta 36 *[2, t. 16.26] Nechť máme $f, g \in \mathbb{F}_q[x]$ polynomy, $k \in \mathbb{N}$. Pak platí*

1. $(f \cdot g)' = f' \cdot g + f \cdot g'$*; speciálně, pokud je například $f(x) = c$ pro nějaké $c \in \mathbb{F}_p$, platí $(f \cdot g)' = f \cdot g'$,*
2. $(f^k)' = k \times f^{k-1} \cdot f'$.

Věta 37 *[2, t. 19.1] Nechť $f \in \mathbb{F}_q[x]$ je nenulový polynom. Pak pokud $\gcd(f, f') = \mathbf{1}$, je f čtvercoprostý.*
Důkaz *Vyplyne z následující úvahy.* ∎

Řekněme, že $f, g, h \in \mathbb{F}_q[x]$ jsou polynomy takové, že pro nějaké $k \in \mathbb{N} \setminus \{1\}$ (které **není** násobkem charakteristiky $\mathbb{F}_q$) platí $f = g^k \cdot h$, g je ireducibilní a $g \nmid h$. Pak $g^{k-1} \mid f'$, neboť

$$(g^k \cdot h)' = k \times g^{k-1} \cdot g' \cdot h + g^k \cdot h'. \tag{4.1}$$

Každý ze sčítanců je dělitelný g^{k-1} beze zbytku, vyšší mocninou už ale ne. Polynom $\gcd(f, f')$ je dělitelný součinem všech ireducibilních činitelů f, ovšem s násobností přesně o 1 menší než jakou mají v rozkladu f. Z toho plyne, že polynom[5] $f_{sf} := \frac{f}{\gcd(f,f')}$ sestává právě z prvních mocnin

[5] sf je zkratka "square free"

všech různých ireducibilních faktorů f. Možnosti jsou nyní dvě - buď rozkládat přímo f_{sf}, a násobnosti činitelů získat zpětně, nebo rozložit rekurzivně stejným postupem polynom $\gcd(f, f')$ a o jeho faktory ponížit f_{sf} - touto cestou se vydáme: největší společný dělitel f_{sf} a $\gcd(f, f')$ sestává právě z těch ireducibilních činitelů f v první mocnině, které v rozkladu f mají násobnost alespoň 2. Označíme-li $d := \gcd(f, f')$, je $e := \frac{f_{sf}}{\gcd(d, f_{sf})}$ produktem jen a pouze těch faktorů f, které mají násobnost 1.

Pokud **je** ale k násobkem charakteristiky tělesa koeficientů daného polynomu, je $k \times g^{k-1} \cdot g' \cdot h$ rovno $\boldsymbol{\theta}$. Potom je ale druhá strana rovnosti 4.1 dělitelná (přinejmenším) k-tou mocninou g, a tudíž $\gcd(f, f')$ je sám o sobě dělitelný g^k. Čtvercoprostá faktorizace $f_{sf} = \frac{f}{\gcd(f, f')}$ tedy g jakožto činitel obsahovat nebude. Platí následující tvrzení:

Věta 38 *Nechť $\mathbb{F}_q$ je těleso s charakteristikou $p \in \mathbb{P}$, $q = p^n$ pro nějaké $n \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$ je monický polynom nenulového stupně takový, že $\gcd(g, g') = g$. Pak existuje $h \in \mathbb{F}_q[x]$ takový, že $h^p = g$, a pokud $g(x) = \sum_{i=0}^{k} a_i x^{ip}$, pak $h(x) = \sum_{i=0}^{k} a_i^{p^{n-1}} x^i$.*

Nalezneme tedy „p-tou“ odmocninu f, polynom h, a ten dále rekurzivně rozkládáme výše popsaným způsobem.

Následující algoritmus [2, Alg. SFD, str. 528], [1, str. 130] shrnuje výše popsané úvahy:

Algoritmus 1: Čtvercoprostý rozklad polynomu

Input: Monický polynom $f \in \mathbb{F}_q[x]$ stupně alespoň 1

Output: Množina všech (po dvou nesoudělných) čtvercoprostých polynomů, spolu s jejich násobností, z rozkladu f

```
1  vysledek = ∅;
2  celkova_mocnina = 1;
3  repeat
4      hloubka_rekurze = 1;
5      d = gcd(f, f') ;                    /* viz poznámka pod popisem algoritmu */
6      f_sf = f/d ;                        /* 'sf' je zkratka 'square free' */
7      while f_sf ≠ jednotkový polynom do
8          f = f/f_sf ;                    /* sniž násobnost všech faktorů f o 1 */
9          vyssi_mocniny = gcd(f, f_sf) ;  /* všechny faktory f, které mají
               násobnost alespoň 2; v tomto produktu ale v první mocnině */
10         e = f_sf/vyssi_mocniny ;        /* všechny faktory f s násobností právě 1 */
11         if e ≠ jednotkový polynom then
12             vysledek = vysledek ∪ {(e, celkova_mocnina · hloubka_rekurze)};
13         end
14         f_sf = vyssi_mocniny;
15         hloubka_rekurze = hloubka_rekurze + 1;
16     end
17     if f ≠ jednotkový polynom then
18         celkova_mocnina = celkova_mocnina · p ;  /* p je charakteristika tělesa
               koeficientů polynomu f */
19         najdi g ∈ F_q[x] takové, že g^p = f ;     /* pomocí tvrzení 38 */
20         f = g;
21     end
22 until f = jednotkový polynom;
23 return vysledek;
```

Co se tohoto algoritmu týká, tak komentář u řádku 5 je trochu delší - d sestává ze všech faktorů f_i s o 1 menší násobností (než mají v f), vyjma těch faktorů, jejichž násobnost je právě nějaká nenulová mocnina charakteristiky p. Explicitně: pokud má nějaký faktor násobnost například $p + 1$, bude zpracován ve *while* cyklu, který díky tomu proběhne (minimálně) p krát! Jeho potenciálními slabinami jsou tedy faktory s velmi vysokou mocninou, která ale není dělitelná charakteristikou tělesa p.

4.1.0.1 Složitost

Spokojíme se s citací [2, t. 20.5] - složitost je

$$O(\mathrm{st}(f)^2 \cdot D + \frac{\mathrm{st}(f) \cdot (\log(q) - 1) \cdot \log(p)}{p} \cdot EXP),$$

kde D, EXP jsou složitosti dělení a mocnění v $\mathbb{F}_q$. První sčítanec se týká "while cyklu"na řádku 7, druhý člen součtu odpovídá kladnému vyhodnocení podmínky na řádku 17.

4.2 Rozklad čtvercoprostých polynomů

Nechť máme libovolný čtvercoprostý polynom $f \in \mathbb{F}_q[x]$ stupně alespoň 2 (konstantní a lineární polynomy jsou nezajímavé - už jsou z definice ireducibilní). Pak pro následující úvahy je kritické toto tvrzení [1, t. 4.1]:

Věta 39 *Buďte $f, g \in \mathbb{F}_q[x]$ polynomy takové, že $h^q \equiv h \mod f$ a f je monický. Pak*

$$f = \prod_{c \in \mathbb{F}_q} \gcd(f, h - c). \tag{4.2}$$

Důkaz *Z definice* gcd *plyne, že libovolný člen produktu na pravé straně 4.2 dělí f, a pokud $c, d \in \mathbb{F}_q : c \neq d$, pak $\gcd(h - c, h - d) = \mathbf{1}$. Tím pádem $\prod_{c \in \mathbb{F}_q} \gcd(f, h - c) \mid f$.*

Z předpokladů máme $h^q - h \equiv \boldsymbol{\theta} \mod f$, neboli $f \mid h^q - h$. Neboť podle 32 je

$$h^q - h = \prod_{c \in \mathbb{F}_q} (h - c)$$

dostáváme $f \mid \prod_{c \in \mathbb{F}_q} (h - c)$, a o to spíš f dělí i výraz $\prod_{c \in \mathbb{F}_q} \gcd(f, h - c)$, což je mimo jiné monický polynom. Máme tedy dva monické polynomy, každý je dělitelem toho druhého - a to je možné jen tehdy, když jsou si rovny. ∎

Najdeme-li tedy nějaký polynom h splňující výše uvedený požadavek, který ještě navrch bude mít stupeň nenulový a ostře menší než-li f, pak máme jistotu, že $\mathrm{st}(\gcd(f, h - c))$ pro všechna $c \in \mathbb{F}_q$ bude ostře menší než-li stupeň f. V celém produktu 4.2 sestrojeném s pomocí h tedy budou vždy **alespoň 2 netriviální faktory** f - které nemusí být nutně ireducibilní. **Berlekampův algoritmus** se zabývá tím, že takovéto polynomy h nalézá. Následující úvaha vede k jeho odvození : nechť $f \in \mathbb{F}_q[x]$ je součinem ireducibilních polynomů $f_1, \ldots, f_k \in \mathbb{F}_q[x]$. Pak vezmeme-li libovolnou k-tici $(c_1, \ldots, c_k) \in {\mathbb{F}_q}^k$ (kterých je právě q^k různých), následující soustava k rovnic 17 má právě jedno řešení $h \in \mathbb{F}_q[x], \mathrm{st}(h) < \mathrm{st}(f)$ [1, str. 131], [2, t. 17.7]:

$$h(x) \equiv c_i \mod f_i(x) \; \forall i \in \{1, \ldots, k\}. \tag{4.3}$$

Platí navíc, že

$$h^q(x) \equiv c_i^q \mod f_i(x) \; \forall i \in \{1, \ldots, k\}, \tag{4.4}$$

což vzhledem k 30 přejde na

$$h^q(x) \equiv c_i \mod f_i(x) \; \forall i \in \{1, \ldots, k\}, \tag{4.5}$$

takže

$$h^q(x) \equiv h(x) \mod f_i(x) \; \forall i \in \{1, \ldots, k\}. \tag{4.6}$$

neboť relace modulo je tranzitivní. Celkově tedy $h^q(x) \equiv h(x) \mod f$ a $\mathrm{st}(h) < \mathrm{st}(f)$. Takových polynomů existuje přesně q^k různých: pro spor buďte $\vec{c}_1, \vec{c}_2$ různé k-tice a $h \in \mathbb{F}_q[x]$ jejich společné řešení. Protože $\vec{c}_1 - \vec{c}_2$ obsahuje alespoň jednu nenulovou složku (řekněme s indexem $j \in \{0, \ldots, k\}$), musí platit

$$\underbrace{h(x) - h(x)}_{=\boldsymbol{\theta}} \equiv \underbrace{c_{1,j} - c_{2,j}}_{\neq \mathbf{0}} \mod f_j(x), \tag{4.7}$$

což ale není možné. Dále libovolný konstantní polynom $h(x) = i \in \mathbb{F}_q$ je řešením 4.3 a jemu odpovídající vektor $\vec{c}$ je roven $(\underbrace{i, \ldots, i}_{k})$.

Najít všechna řešení 4.6 je jednoduché - označme $h(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$, kde $\mathrm{st}(f) = n+1$. Podle 30 a 6 je $h^q(x) = a_0 + a_1 \cdot x^q + \ldots + a_n \cdot x^{qn}$. Každou mocninu x zredukujeme modulo $f(x)$ a získáme tak $n+1$ polynomů $b_i \in \mathbb{F}_q[x]$, $\mathrm{st}(b_i) < \mathrm{st}(f)$:

$$x^{qi} \equiv b_i(x) \mod f(x) \; \forall i \in \{0, 1, \ldots, n\}. \tag{4.8}$$

Dosazením do 4.6 získáváme

$$a_0 b_0(x) + a_1 b_1(x) + \ldots + a_n b_n(x) \equiv a_0 + a_1 x + \ldots + a_n x^n \mod f(x), \tag{4.9}$$

a neboť stupně polynomů na obou stranách jsou ostře menší než stupeň f, jsou si rovny, neboli mají identické koeficienty u stejných mocnin x. Označme $b_{j,i} \in \mathbb{F}_q$ koeficient u x^j v polynomu b_i. Pak přímým porovnáním koeficientů u oněch stejných mocnin x získáváme

$$\sum_{k=0}^{n} a_k b_{j,k} = a_j \; \forall j \in \{0, 1, \ldots, n\}. \tag{4.10}$$

Tyto soustavy lze shrnout maticově:

$$\begin{pmatrix} b_{0,0} & \dots & b_{0,n} \\ \vdots & \ddots & \vdots \\ b_{n,0} & \dots & b_{n,n} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix},$$

nebo-li

$$\underbrace{\begin{pmatrix} b_{0,0} & \dots & b_{0,n} \\ \vdots & \ddots & \vdots \\ b_{n,0} & \dots & b_{n,n} \end{pmatrix}}_{\mathbb{B}} \cdot \underbrace{\begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix}}_{\vec{a}} - \underbrace{\begin{pmatrix} \mathbf{1} & \dots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \dots & \mathbf{1} \end{pmatrix}}_{\mathbb{I}} \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix}}_{\vec{\mathbf{0}}},$$

což lze kompaktněji zapsat jako

$$(\mathbb{B} - \mathbb{I})\,\vec{a} = \vec{\mathbf{0}}. \tag{4.11}$$

Libovolné řešení této maticové soustavy, to jest vektor $\vec{a}$, převedeme na polynom velmi jednoduše: i-tá složka vektoru odpovídá koeficientu u x^{i-1}. Formálně můžeme polynom získat také vynásobením pseudo-maticí rozměru $1 \times (n+1)$ zleva:

$$\begin{pmatrix} x^0 & x^1 & x^2 & \dots & x^n \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = h(x)$$

Zpět k soustavě 4.11 - množina jejích řešení H je vektorový podprostor (prostoru ${\mathbb{F}_q}^{n+1}$ nad $\mathbb{F}_q$ s operacemi + a · definovanými po složkách). Vzhledem k tomu, že pravá strana je nulový vektor, platí $H = \ker(\mathbb{B} - \mathbb{I})$. Víme, že existuje právě q^k řešení, jak plyne z úvah počínaje 4.3 a konče 4.7, takže H musí sestávat z q^k vektorů, jeho báze je tedy z k prvků, což je rovno počtu

ireducibilních faktorů polynomu f. Celý postup [1, str. 132] je shrnut v následujícím algoritmu:

Algoritmus 2: Nalezení f-redukujících polynomů

Input: Monický polynom $f \in \mathbb{F}_q[x]$ stupně alespoň 1

Output: Báze vektorového prostoru všech polynomů $h \in \mathbb{F}_q[x]$ takových, že $h^q \equiv h \mod f$ a zároveň $\mathrm{st}(h) < \mathrm{st}(f)$

1 *vysledek* $= \emptyset$;
2 $n = \mathrm{st}(f)$;
3 pro $\forall i \in \{0, 1, \ldots, n\}$ vygeneruj polynomy $b_i \in \mathbb{F}_q[x]$ takové, že $x^{i \cdot q} \equiv b_i(x) \mod f(x)$;
4 vytvoř čtvercovou matici $\mathbb{B}$ z prvků $\mathbb{F}_q$ takovou, že na pozici (i, j) se nachází koeficient x^{i-1} polynomu b_{j-1} ; `/* matice je řádu` $n+1$`, a indexujeme jí zde od` $(1,1)$ `*/`
5 urči bázi jádra matice $(\mathbb{B} - \mathbb{I})$; `/* například Gaussovo eliminací */`
6 každý bazický vektor převeď na polynom: i-tá složka je koeficient u x^{i-1} - tento polynom vlož do množiny *vysledek*;
7 **return** *vysledek;*

4.2.0.1 Složitost Nechť $f \in \mathbb{F}_q[x]$ má stupeň $n + 1 \in \mathbb{N}$. Pak nalézt polynom b_1 definovaný na řádku 3 algoritmu 2 lze pomocí exponenciace v $\mathbb{F}_q[x]$ a redukce modulo f po každém kroku, což dává $O(\log(q)\,\mathrm{st}(f)^2(M + D))$ pro M, D složitost operace násobení a redukce modulem v $\mathbb{F}_q$. Libovolné další b_i lze získat rekurzivně:

$$b_i = b_1 \cdot b_{i-1} \mod f. \tag{4.12}$$

Cena této operace je $O(\mathrm{st}(f)^2(M + D))$, a bude provedena celkem $n - 1$ krát, takže celkově máme složitost $O((\log(q) + \mathrm{st}(f) - 1)\,\mathrm{st}(f)^2(M + D))$, kde platí $\mathrm{st}(f) = n + 1$.

Vytvoření matice soustavy znamená jen přečtení/nakopírování n^2 prvků v paměti, kdy každý má velikost maximálně $\log(q)$. Gaussova eliminace vyžaduje řádově $O(n^3)$ operací sčítání a násobení, což dává $O(n^3(M + A))$, kde M a A jsou složitosti operací $\cdot$ a $+$ v $\mathbb{F}_q$. Označíme-li $\dim \ker(\mathbb{B} - \mathbb{I}) = k$, pak zpětná substituce vyžaduje $O(kn^2)$ násobení a sčítání v $\mathbb{F}_q$, ale i $O(kn)$ nalezení inverzních prvků v $\mathbb{F}_q$.

Převod vektorů na polynomy je zanedbatelný.

V [2, t. 20.10] se uvádí složitost $O(\mathrm{st}(f)^3 + \mathrm{st}(f)^2 \cdot \log(q))$ **operací v tělese** $\mathbb{F}_q$. Naše úvaha má i tyto složitosti rozepsané pro přiloženou implementaci.

Věta 40 *První fáze Berlekampova algoritmu 2 má složitost rovnu součtu všech výše uvedených. Dominantní je nalezení všech vektorů b_i se složitostí $O((\log(q) + n)n^2(M + D))$.*

Nyní popíšeme dvě možnosti, jak rozložit f pomocí báze nalezené algoritmem 2. Nejdříve ale dokážeme tvrzení, které se nám bude v obou případech hodit [1, str. 133]:

Věta 41 *Nechť $f \in \mathbb{F}_q[x]$ je monický čtvercoprostý polynom, $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ jsou všechny jeho ireducibilné činitelé a $M = \{h_1, \ldots, h_k\}$ je polynomiální báze nalezená algoritmem 2. Pak*

pro $\forall f_i, f_j : f_i \neq f_j$ *existuje polynom* $h \in M$ *takový, že* $f_i \mid \gcd(h-c, f) \wedge f_j \mid \frac{f}{\gcd(h-c,f)}$ *pro nějaké* $c \in \mathbb{F}_q$.

Důkaz *Víme, že 4.6 má* q^k *unikátních řešení. Ke každému takovému* h *existuje* $\vec{c} \in {\mathbb{F}_q}^k$ *takový, že splňuje 4.3. Cheme-li separovat, bez újmy na obecnosti,* f_1 *a* f_2*, pak dozajista existuje* k*-tice (definující polynom skrze 4.3) která má první složku* $\mathbf{0}$ *a druhou* $\mathbf{1}$*. K této* k*-tici existuje unikátní* $h \in \mathbb{F}_q[x]$*, a ten je lineární kombinací vektorů z* M *s koeficienty* $a_1, \ldots, a_k \in \mathbb{F}_q$ *- zaměříme-li se na první* 2 *rovnice, máme*

$$\begin{aligned} a_1 \cdot h_1(x) + \cdots + a_k \cdot h_k &\equiv \mathbf{0} \mod f_1(x) \\ a_1 \cdot h_1(x) + \cdots + a_k \cdot h_k &\equiv \mathbf{1} \mod f_2(x), \end{aligned}$$

což implikuje, že alespoň jeden ze všech polynomů h_i *(jeho index budiž* n*), jejichž koeficienty* a_i *jsou nenulové, musí být určen* k*-ticí s první a druhou složkou různou, označme je například* $s_1, s_2 \in \mathbb{F}_q$*. Pak ale* $f_1 \mid \gcd(f, h_n - s_1)$ *a* $f_2 \nmid \gcd(f, h_n - s_1)$ *což spolu s* $\gcd(h_n - s_1, h_n - s_2) = \mathbf{1}$ *dává tvrzení věty.* ∎

4.2.1 Deterministická faktorizace pomocí sestrojené báze

Algoritmus [1, str. 132] je následující:

Algoritmus 3: Deterministický rozklad f

Input: Monický a čtvercoprostý polynom $f \in \mathbb{F}_q[x]$ stupně alespoň 1

Output: Rozklad f na ireducibilní činitele

```
1  vysledek = {f};
2  H = množina polynomů získaná algoritmem 2;
3  if |vysledek| ≠ |H| then
4      foreach h ∈ H do
5          if h je jednotkový polynom then
6              continue;        /* jednotkový polynom neseparuje žádné faktory f */
7          else
8              foreach c ∈ F_q do
9                  foreach d ∈ vysledek do
10                     g = gcd(d, h − c);
11                     if g je netriviální dělitel d then
12                         vysledek = vysledek \ {d};        /* odeber složený polynom */
13                         vysledek = vysledek ∪ {d/g, g};        /* ulož jeho činitele */
14                         if |vysledek| = |H| then
15                             return vysledek;
16                         end
17                     end
18                 end
19             end
20         end
21     end
22 else
23     return vysledek;                                        /* f je ireducibilní */
24 end
```

Díky větě 41 vrátí po konečném počtu kroků správný výsledek. Ale jaký je tento počet kroků? Úměrný řádu $\mathbb{F}_q$, to jest číslu q. Detailněji:

Věta 42 (Složitost) *Komplexita algoritmu 3 je $O(qkD)$, kde $k = \dim H$ a D je složitostí euklidova algoritmu v $\mathbb{F}_q[x]$, neboli celkově $O(qk\,\mathrm{st}(f)^2(M+I))$ pro M, I cenu spočtení součinu a inverze v $\mathbb{F}_q$.*

Důkaz *Nejhorší možná situace je ta, že každé nejednotkové $h \in H$ rozdělí f_p pouze na dva faktory pro poslední zkoušené c z hlavičky '**foreach**' cyklu na řádku 8. Takto bude probrána celá*

*množina H, která má $k-1$ nekonstantních prvků. V i-té iteraci cyklu '**foreach**' na řádku 4 se bude počítat* gcd *pro $i-1$ polynomů. Tím dostáváme pesimistický horní odhad $O(q(k-1)^2 D)$.*

Spodní odhad je oproti tomu $O(kD)$, nebo-li když ke všem rozdělením dojde při prvních $k-1$ příležitostech.

*Jaký je ale průměrný potřebný počet iterací? S pravděpodobností $\frac{q(q-1)\ldots(q-k+1)}{q^k}$, což je pro k řádově menší než q velmi blízko 1, dojde ke všem rozdělením hned v první iteraci '**foreach**' z řádku 4, ale i tak bude potřeba projít řádově q prvků tělesa $\mathbb{F}_q$, což dává $O(qD)$. Pokud je q řádově větší než-li k, neuděláme velkou chybu, pokud napíšeme $O(qkD)$ namísto $O(qD)$. Zároveň jsme tak pokryli i případ, kdy jsou obě čísla řádově blízká.* ∎

V důkazu bylo využito toho, že složky vektoru $\vec{c}$, určené 4.3, jsou nezávislé náhodné veličiny s rovnoměrným rozdělením.

Zdůrazněme, že skoro ve všech složitostech popsaných algoritmů se nachází $\log(q)$, zde však q. Má smysl nad ním uvažovat, jen pokud je q stejného řádu jako k. Pro „velká“ q je lepší následující algoritmus:

4.2.2 Nedeterministická faktorizace pomocí sestrojené báze

Algoritmus [2, Alg. B2], který zde popíšeme, závisí na náhodných číslech - proto přízvisko nedeterministický, nicméně vrácený výsledek je rozhodně vždy správný - náhoda spočívá pouze v tom, po kolika krocích se jej dobereme.

Idea je následující: díky 4.2 pro nekonstantní polynomy h stupně ostře menšího než $\mathrm{st}(f)$ platí

$$f(x) \mid h^q(x) - h(x), \tag{4.13}$$

což je produkt polynomů $(h(x)-c)$ pro všechna různá $c \in \mathbb{F}_q$ majících tu vlastnost, že $c \neq d \Rightarrow \gcd(h(x)-c, h(x)-d) = \mathbf{1}$. Pokud je $f \in \mathbb{F}_q[x]$ reducibilní, podle věty 41 alespoň 2 členy produktu budou mít netriviálního společného dělitele s f.

V případě, že q je liché, platí následující rovnost:

$$h^q - h = h \cdot \left(h^{\frac{q-1}{2}} - \mathbf{1}\right) \cdot \left(h^{\frac{q-1}{2}} + \mathbf{1}\right). \tag{4.14}$$

Pokud je q mocnina 2 (což nutně znamená, že $\mathbb{F}_q$ má charakteristiku 2), řekněme $q = 2^m$, pak $h^q - h$ takhle jednoduše rozložit nejde - ale přeci jen možnost, jak jej rozdělit na 2 polynomy stejného stupně, existuje. Pro libovolné $a, b \in \mathbb{F}_{2^m}[x]$ platí $(a+b)^2 = a^2 + b^2$, neboť

$$a^2 + a \cdot b + b \cdot a + b^2 = a^2 + \underbrace{2 \times a \cdot b}_{=\mathbf{0}} + b^2. \tag{4.15}$$

Velmi jednoduše lze ukázat, že $(a+b+\cdots+z)^2 = a^2+b^2+\cdots+z^2$ pro $\forall a,b,\ldots,z \in \mathbb{F}_{2^m}[x]$. Vezměme nyní výraz $tr(h) = \sum_{i=0}^{m-1} h^{2^i}$ a spočtěme jeho čtverec:

$$tr^2(h) = (h^{2^{m-1}} + \cdots + h^4 + h^2 + h)^2 = h^{2^m} + h^{2^{m-1}} + \cdots + h^8 + h^4 + h^2. \tag{4.16}$$

Přičteme-li k pravé straně rovnosti $tr(h)$, získáváme

$$h^{2^m} + \underbrace{2 \times h^{2^{m-1}}}_{=\mathbf{0}} + \cdots + \underbrace{2 \times h^8}_{=\mathbf{0}} + \underbrace{2 \times h^4}_{=\mathbf{0}} + \underbrace{2 \times h^2}_{=\mathbf{0}} + h = h^{2^m} + h, \tag{4.17}$$

což je přesně kýžený cíl:

$$h^{2^m} - h = h^{2^m} + h = tr(h) \cdot (tr(h) + \mathbf{1}). \tag{4.18}$$

Tyto částečné faktorizace jsou výhodné pro rokládání polynomu f - rozdělují totiž všechny polynomy, které potenciálně mají netriviální největší společný dělitel s f, do 2, respektive 3, částí [2, t. 20.7 a 20.8]:

Věta 43 *Nechť $f \in \mathbb{F}_q[x]$ je reducibilní polynom a M soubor polynomů získaný algoritmem 2. Pak pro $\forall h \in \mathbb{F}_q[x]$, nenulovou lineární kombinací vektorů z M, je $\gcd(S(h), f)$ netriviálním dělitelem f s pravděpodobností*

1. $1 - (\frac{1}{2})^{|M|-1}$, *pokud je $q = 2^m$ pro nějaké $m \in \mathbb{N}$ a $S(h) = tr(h)$,*
2. $1 - \left(\frac{q-1}{2q}\right)^{|M|} - \left(\frac{q+1}{2q}\right)^{|M|}$ *pro q liché a $S(h) = h^{\frac{q-1}{2}} + \mathbf{1}$.*

Důkaz *Nechť $f_1,\ldots,f_k \in \mathbb{F}_q[x]$ jsou všechny ireducibilní faktory f. Pak pro každé h existuje k-tice $\vec{c} = (c_1,\ldots,c_k) \in {\mathbb{F}_q}^k$ splňující 4.3. Pokud*

1. *je q sudé, pravděpodobnost toho, že $h(x) - c_i$ je faktorem $tr(h)$, je rovna $\frac{q}{2q} = \frac{1}{2}$. Pravděpodobnost toho, že $\gcd(h(x) - c_i, tr(h)) \neq \mathbf{1}$ pro $\forall i \in \{1,\ldots,k\}$, je $\left(\frac{1}{2}\right)^k$, potom ale $\gcd(f, tr(h)) = f$. Úplně stejnou úvahou se dojde k tomu, že $\gcd(h(x) - c_i, tr(h)) = \mathbf{1}$ pro $\forall i \in \{1,\ldots,k\}$, což znamená $\gcd(f, tr(h)) = \mathbf{1}$, se stane s pravděpodobností $\left(\frac{1}{2}\right)^k$, takže pravděpodobnost triviálního největšího společného dělitele je $2\left(\frac{1}{2}\right)^k$, a opak, to jest nalezení netriviálního největšího společného dělitele, nastane s pravděpodobností $1 - \left(\frac{1}{2}\right)^{k-1}$;*
2. *je q liché, úvaha je podobná jako v předchozím bodě, nebo-li $\gcd(h(x) - c_i, S(h)) \neq \mathbf{1}$ nastane s pravděpodobností $\frac{\frac{q-1}{2}}{q} = \frac{q-1}{2q}$, naopak $\gcd(h(x) - c_i, S(h)) = \mathbf{1}$ nastane s pravděpodobností $1 - \frac{q-1}{2q} = \frac{2q-q+1}{2q} = \frac{q+1}{2q}$. Pravděpodobnost toho, že všichni činitelé budou mít za největší společný dělitel spolu s $S(h)$ nejednotkový, respektive jednotkový, polynom, je $\left(\frac{q-1}{2q}\right)^k$, respektive $\left(\frac{q+1}{2q}\right)^k$. Netriviální největší společný dělitel nastane tedy s pravděpodobností $1 - \left(\frac{q-1}{2q}\right)^k - \left(\frac{q+1}{2q}\right)^k$.*

Vzhledem k tomu, že $k = |M|$, tvrzení je dokázáno. ∎

Věta je sice dokázána pro f, nicméně pro součin libovolné j-prvkové podmožiny všech faktorů f je stále platná s koeficientem j namísto $|M|$. Opět se předpokládá, že složky vektoru $\vec{c}$, určené 4.3, jsou nezávislé náhodné veličiny s rovnoměrným rozdělením.

Zjednodušeně rečeno, polynom $h^{2^m}(x) - h(x) \in \mathbb{F}_{2^m}[x]$ je rozložen na součin 2 polynomů stejného stupně - každý z nich obsahuje tedy přesně polovinu (nějakých a vesměs různých) činitelů $h(x) - c$ pro všechna $c \in \mathbb{F}_{2^m}$; pro q liché je situace téměř stejná - až na faktor $h(x) - \mathbf{0}$, který je třetím činitelem. Spodní odhady těchto pravděpodobností jsou

1. $\frac{1}{2}$ pro q sudé a $k = 2$,
2. $\frac{4}{9}$ pro q liché - výraz je z hlediska q pro fixní k minimální pro $q = 3$, a naopak pro fixní q je minimimální pro $k = 2$.

Možnost $k = 1$, to jest f je ireducibilní, nemá smysl uvažovat.

Algoritmus je následující:

Algoritmus 4: Nedeterministický rozklad f

Input: Monický a čtvercoprostý polynom $f \in \mathbb{F}_q[x]$ stupně alespoň 1

Output: Rozklad f na ireducibilní činitele

```
1  vysledek = {f};
2  H = množina polynomů získaná algoritmem 2;
3  if |vysledek| ≠ |H| then
4  |  if q = 2^m then
5  |  |  S(h) = tr(h);
6  |  else
7  |  |  S(h) = h^((q−1)/2) + 1;
8  |  end
9  |  foreach d ∈ vysledek do
10 |  |  h = náhodná nenulová lineární kombinace prvků H;
11 |  |  g = gcd(d, S(h));
12 |  |  if g je netriviální dělitel d then
13 |  |  |  vysledek = vysledek \ {d};          /* odeber složený polynom */
14 |  |  |  vysledek = vysledek ∪ {d/g, g};      /* ulož jeho činitele */
15 |  |  |  if |vysledek| = |H| then
16 |  |  |  |  return vysledek;
17 |  |  |  end
18 |  |  end
19 |  end
20 else
21 |  return vysledek;                           /* f je ireducibilní */
22 end
```

Pravděpodobnost, že netriviální největší společný dělitel dostaneme přesně po l iteracích, je $p \cdot (1-p)^l$, kde p je pravděpodobnost určená větou 43. Střední hodnota počtu operací l je $\frac{1-p}{p}$, a vzhledem k tomu, že $p \geq \frac{4}{9}$, je střední počet k faktorizaci nevedoucích iterací nejvýše $\frac{5}{4}$, takže, statisticky vzato, k úspěchu dojde v $2,25$-té iteraci. Po každém rozdělení počítáme sice jeden největší společný dělitel navíc, ale zato s polynomy menšího stupně. Protože pro libovolné $a, b, k \in \mathbb{N}$ platí $a^k + b^k \leq (a+b)^k$, počítání více vnitřních iterací s polynomy menších stupňů nikdy nebude vyžadovat ostře víc operací, nežli počítat s polynomem stupně rovného jejich součtům. Potřebujeme provést právě $k-1$ rozdělení různého počtu polynomů, jejichž stupně dávají v součtu stupeň f, což podle předchozí úvahy nebude stát víc nežli $k-1$ provedených iterací (nehledě na výsledek) s f. Konkrétně střední hodnota počtu iterací nutných k dosažení výsledku bude nanejvýš $2,25(k-1)$.

Složitost jedné iterace je součtem

1. vygenerování polynomu h, náhodné lineární kombinace k polynomů, čehož lze dosáhnout v $O(k \log(q) A)$ operacích pro A cenu sečtení dvou prvků $\mathbb{F}_q$,

2. spočtení $S(h)$, což pomocí binárního umocňování modulo f stojí $O(\log(q)\,\mathrm{st}(f)^2(M+I))$ pro M, I složitosti násobení a najití inverze v $\mathbb{F}_q$,

3. zjištění největšího společného dělitele, což dává $O(\mathrm{st}(f)^2(M+I))$,

4. a v případě netriviálního dělitele i jedno dělení polynomů, které stojí $O(\mathrm{st}(f)^2(M+I))$.

Dominantní je rozhodně spočtení $S(h)$. Spolu s úvahou výše můžeme tedy tvrdit, že střední hodnota počtu operací je přinejhorším $O(k \log(q)\,\mathrm{st}(f)^2(M+I))$, což je z hlediska q o mnoho lepší výsledek než-li $O(qk\,\mathrm{st}(f)^2(M+I))$ pro $q \geq 2$. Ovšem pro malá q může hrát roli konstantní koeficient před celým výrazem, který se v zápisu $O(\cdot)$ vynechává, popřípadě další v $O(\cdot)$ nedominantní členy.

4.3 Berlekampův algoritmus

Pospojováním všeho předchozího dostáváme **Berlekampův algoritmus**:

Algoritmus 5: Berlekampův algoritmus

Input: Monický polynom $f \in \mathbb{F}_q[x]$ stupně alespoň 1

Output: Všechny ireducibilní činitele spolu s jejich násobností v rokladu f

```
1 vysledek = ∅;
2 SF = množina všech čtvercoprostých činitelů f získaná algoritmem 1;
3 foreach f_sf ∈ SF do
4 |   pow = násobnost f_sf v rozkladu f;
5 |   rozklad = rozklad f_sf získaný deterministickým 3 nebo pravděpodobnostním 4
  |     algoritmem;
6 |   vysledek = vysledek ∪ {(rozklad, pow)};
7 end
8 return vysledek;
```

Jeho složitost je součtem dílčích částí, explicitně:

- algoritmus 1 má složitost $O(\mathrm{st}(f)^2 \cdot D)$, nebo-li pouze úměrnou složitosti hledání největších společných dělitelů v $\mathbb{F}_q[x]$, což je oproti následujícím částem zanedbatelné,
- při hledání polynomů tvaru 4.6 v 2 je nejdražší binární umocňování a redukce modulem v $\mathbb{F}_q[x]$, složitost je $O((\log(q)+n)n^2(M+I))$,
- k rozbíjení f na ireducibilní činitele můžeme využít jeden ze dvou algoritmů:

  1. algoritmus 3 o složitosti $O(qk\,\mathrm{st}(f)^2(M+I))$,

2. nebo nedeterministický 4, jež potřebuje řádově $O(\log(q)k\,\mathrm{st}(f)^2(M+I))$ operací pro dokončení faktorizace.

Neboť $\mathrm{st}(f) = n$, celkové složitosti dominuje (pouze o faktor k, počet po dvou různých ireducibilních činitelů f) druhá fáze. Proto má Berlekampův algoritmus složitost při nejlepším $O(\log(q)k\,\mathrm{st}(f)^2(M+I))$. Pokud je ale f ireducibilní, zastaví se hned po první fázi, a složitost zůstává stejná.

5 Závěr

V této bakalářské práci jsme se věnovali faktorizaci polynomů nad konečným tělesem pomocí Berlekampova algoritmu. K této práci je přiložena jeho implementace v jazyce C++. Je značně omezená, neboť za tělesa koeficientů lze brát pouze $\mathbb{F}_q$, to jest Galoisova tělesa řádu q, což je mocnina libovolného prvočísla p. V případě mocniny $k \geq 1$ nelze poskytnout obecné těleso řádu p^k, nýbrž jen $\mathbb{F}_p/_{\langle f \rangle}$, což je těleso polynomů modulo ireducibilní polynom $f \in \mathbb{F}_p$ stupně právě k.

Do budoucna by se šlo zaměřit na větší obecnost napsaného kódu, zrychlení interních algoritmů modulární i polynomiální aritmetiky a případného naimplementování jiných algoritmů řešících tuto úlohu.

Literatura

[1] Rudolf Lidl, Harald Niederreiter: *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986

[2] Victor Shoup: *A Computational Introduction to Number Theory and Algebra*, https://www.shoup.net/ntb/ntb-v2.pdf, přístup 4.4.2019

[3] Jan Mareš: *Algebra*, České Vysoké Učení Technické v Praze, 2014

[4] John Maddock, Christopher Kormanyos: *Boost multiprecision library*, https://www.boost.org/, přístup 30.4.2019